CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6
DISTRIBUTION: A, B, C, J, S

CJCSI 6211.02B
31 July 2003

DEFENSE INFORMATION SYSTEM NETWORK (DISN): POLICY, RESPONSIBILITIES AND PROCESSES

References: Enclosure D.

1. Purpose. This instruction establishes policy, responsibilities and connection approval process for sub networks of the Defense Information System Network (DISN). Additional overall and specific policies governing other sub networks of the DISN are covered in the following instructions:

a. CJCSI 6250.01A, "Satellite Communications" (reference a).

b. CJCSI 6215.01B, "Policy for Department of Defense Voice Networks" (reference b).

c. Director of Central Intelligence Directive (DCID) 6/3, "Protecting Sensitive Compartmented Information within Information Systems" (reference c).

2. Cancellation. CJCSI 6211.02A, 22 May 1996, "Defense Information System Network and Connected Systems," is canceled.

3. Applicability. This instruction applies to the Joint Staff, combatant commands, Services, Defense Agencies, Department of Defense (DOD) field activities and joint activities; including DOD and Service Nonappropriated Fund Instrumentalities.

4. Policy. Enclosure A.

5. Definitions. See Glossary.

6. Responsibilities. Enclosure B.

7. Summary of Changes

a. This new version focuses on DISN policy and responsibilities with additional emphasis on processes for assured connection of unclassified and classified information systems.

b. Provides guidance on the DISN Information Assurance Program (Enclosure C).

c. Provides guidance on cross domain connections between security domains (i.e., internal to DOD and foreign) and cross functional connections with non-DOD organizations (e.g., non-DOD USG agencies and contractor) (Enclosure C).

d. Provides guidance on DISN Video Services (DVS) Connection Requests (Enclosure C).

8. Releasability. This instruction is approved for public release; distribution is unlimited. DOD components (to include the combatant commands), other Federal agencies, and the public may obtain copies of this instruction through the Internet from the CJCS Directives Home Page--http://www.dtic.mil/doctrine. Copies are also available through the Government Printing Office on the Joint Electronic Library CD-ROM.

9. Effective Date. This instruction is effective immediately.

For the Chairman of the Joint Chiefs of Staff:

JAMES A. HAWKINS
Major General, USAF
Vice Director, Joint Staff

Enclosures
- A - Policy
- B - Responsibilities
- C – Connection Process
- D - References
- GL - Glossary

DISTRIBUTION

Distribution A, B, C, and J plus the following:

	Copies
Assistant Secretary of Defense (Networks and Information Integration (NII))	2

(INTENTIONALLY BLANK)

LIST OF EFFECTIVE PAGES

The following is a list of effective pages. Use this list to verify the currency and completeness of the document. An "O" indicates a page in the original document.

PAGE	CHANGE	PAGE	CHANGE
1 thru 2	O	C-C-A-1 thru C-C-A-2	O
i thru x	O	C-C-B-1 thru C-C-B-2	O
A-1 thru A-8	O	C-C-C-1 thru C-C-C-4	O
B-1 thru B-18	O	C-D-1 thru C-D-4	O
C-1 thru C-2	O	C-D-A-1 thru C-D-A-4	O
C-A-1 thru C-A-16	O	C-E-1 thru C-E-6	O
C-B-1 thru C-B-4	O	D-1 thru D-2	O
C-C-1 thru C-C-6	O	GL-1 thru GL-10	O

(INTENTIONALLY BLANK)

RECORD OF CHANGES

Change No.	Date of Change	Date Entered	Name of Person Entering Change

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

Page

ENCLOSURE A--POLICY

ENCLOSURE B--RESPONSIBILITIES

APPENDIX A--SIPRNET CONNECTION REQUESTS

APPENDIX B--NIPRNET CONNECTION REQUESTS

GLOSSARY

FIGURE

TABLE

(INTENTIONALLY BLANK)

ENCLOSURE A

POLICY

1. DISN Background

a. The DISN is DOD's component for the Global Information Grid (GIG) providing a worldwide network that allows the warfighter to exchange information in a seamless, interoperable and global battlespace. Its underlying infrastructure is composed of three major segments or blocks:

(1) The sustaining base (i.e., base, post, camp or station and Service Enterprise Networks) command, control, communications, computers and intelligence (C4I) infrastructure will interface with the long-haul network to support the deployed warfighter. The sustaining base segment is primarily responsibility of Services.

(2) The long-haul telecommunications infrastructure, which includes the communication systems and services between the fixed environment and the deployed joint task force (JTF) and/or coalition task force (CTF) warfighter. The long-haul telecommunications infrastructure segment is primarily responsibility of Defense Information Systems Agency (DISA).

(3) The deployed warfighter and associated combatant commander telecommunications infrastructures supporting the JTF and/or CTF. The deployed warfighter and associated combatant command telecommunications infrastructure is primarily responsibility of Services.

b. The DISN infrastructure is an integrated network, centrally managed and configured to provide dedicated bandwidth, voice, data and video services in support of national defense C4I decision support requirements.

c. The DISN provides the GIG transfer infrastructure by integrating separate combatant command, Service and Agency (CC/S/A) networking requirements into a DOD enterprise-wide network to meet common-user and special purpose information transfer requirements.

d. DISN information transfer facilities support secure transport requirements for sub networks such as the Defense Switch Network (DSN), Defense Red Switch Network (DRSN), Non-Classified Internet Protocol Router Network (NIPRNET), SECRET Internet Protocol Router

Network (SIPRNET)), DISN Video Services Global (DVS-G) Network and the Joint Worldwide Intelligence Communications System (JWICS).

2. DISN Required Features

a. Global in scope.

b. Interoperable between all infrastructure segments or blocks.

c. Support multiple information transfer services for DOD users, including:

(1) point-to-point and point-to-multipoint;

(2) switched voice and data, currently DSN/DRSN, NIPRNET and SIPRNET; and

(3) video services.

d. Capable of rapid expansion or reconfiguration (minutes and hours) and extension to the tactical environment, and be interoperable with tactical systems. Bandwidth capacity for surge will be engineered and allocated based on contingency requirements and Joint Staff validation and direction.

e. Support automatic rerouting and restoral of circuits by priority IAW with existing national security emergency preparedness (NSEP) procedures, telecommunications service priority (TSP) procedures, and other procedures as required to ensure network performance and user requirements are met.

f. Operation, maintenance and management under the full control of military and DOD civilian personnel.

g. Robust, adaptive and reliable by employing network and configuration management, diverse routing and automatic rerouting features.

h. Sub network and component survivability commensurate with the supported command or mission.

i. Support multilevel precedence and preemption (to meet assured connectivity requirements) and all classifications of information.

j. Support value-added services, such as messaging and conferencing, and allow for the addition of new services and technologies.

k. Provide a secure information environment for the processing, storage, transfer and use of information IAW the DISN security policy.

l. Capable of detecting attempts to access the network by unauthorized users. Support automatic denial of such access attempts and automated reporting of such attempts to the DISN management structure.

3. Policy

a. All DOD long-haul communications requirements will be submitted to DISA IAW DODI 4640.14 (reference d). DISA will use the appropriate DISN service to satisfy DOD long-haul and wide-area network information transfer requirements. Sustaining base and deployable segment requirements will be processed IAW reference d and the supporting components' procedures.

b. All connections will follow connection approval procedures and processes, as established in this instruction. This includes requests for cross domain connection of TOP SECRET information systems or any other networks (e.g., Secret, Confidential, Unclassified or Coalition) either directly or indirectly to the DISN.

c. Connections must be designed, developed, integrated, certified and accredited in compliance with of the DOD Information Technology Security Certification and Accreditation Process (DITSCAP) and documented in a System Security Authorization Agreement (SSAA) IAW DOD Directive 8500.1 (reference e) and DOD Instruction 5200.40 (reference f) and DOD 8510.1-M (reference g).

d. Secure configurations of approved information assurance (IA) and IA-enabled information technology (IT) products, uniform risk criteria, trained systems security personnel and strict configuration control will be used for DISN.

e. The DISN designated approving authorities (DAAs) will establish procedures to assess community risk and the measures taken to mitigate risk.

(1) Applications, systems or networks (e.g., Global Command and Control System (GCCS) or DSRN) that will be deployed to multiple enclaves connected to the DISN will be assessed for security features and

community risk.

(2) Applications, systems or networks that have not completed assessments may only be deployed on operational networks with specific site and DISN DAA approval as an exception. Such deployments will be of limited duration and focus on development of operational usage guidelines and procedures based on specific DISN DAA approval conditions and restrictions.

f. All connections of information systems will be managed to continuously minimize community risk by ensuring the assurance of one system is not undermined by vulnerabilities of interconnected systems.

g. Information provided through connections must be released IAW DOD 5200.1-R (reference h), DOD Directive 5230.11 (reference i), and CJCSI 5221.01 (reference j).

h. Connection among information systems of different security domains (e.g., different classification levels, formal compartments, DOD with non-DOD entities) will be IAW DOD Directive 8500.1 (reference e), DOD Instruction 8500.2 (reference k) and DOD Instruction 8540.aa (reference l). As a condition of approval, such connection devices must have an identified program management structure that retains configuration management responsibility for all deployed systems throughout their operational life-cycle.

(1) Connections among DOD information systems of different security domains, with other non-DOD US Government systems, contractor systems of different security domains will be used only to meet compelling operational requirements, not convenience.

(2) The connection of DOD information systems with those of US allies, foreign nations, coalition partners, international organizations, non-DOD government agencies and contractors must be validated by the Joint Staff and approved by Joint Staff or Office of the Secretary of Defense (OSD) prior to initiating connection actions (See Appendix D to Enclosure C). Connections must follow applicable international agreements and comply with DOD Directive 8500.1 (reference e) and CJCSI 6510.01 (reference m). Final approval by DISN DAAs is required before final connection.

(3) The connection of TOP SECRET information systems to a different security domain within the DISN must be approved by the DISN DAAs and comply with applicable security directives and instructions

(DOD Instruction 8500.2 (reference k)).

(4) Because these cross domain connections are considered high risk, the enclave DAA will revalidate the operational basis of the information transfer requirement, recertify and reaccredit the solution annually. Recertification will include an independent vulnerability assessment of the connection (i.e., assessment by an organization not directly responsible for connection).

(5) Only cross domain solutions (i.e., process limiting the exchange of information between systems) approved by the DISN DAAs may be used to connect information systems of different security domains.

(6) The operational requirements and information protection requirements for all connections between different security domains must be validated prior to development of engineering solutions. Procedures within the DITSCAP process, including review of connections as part of the community-wide technical risk assessment by Cross Domain Technical Advisory Board (CDTAB) for approval by the DISN Security Accreditation Working Group (DSAWG) must be followed.

i. The four DISN DAAs (Director, Joint Staff; Director, DISA; Director, Defense Intelligence Agency (DIA); and Director, National Security Agency (NSA)) hold the responsibility for reviewing and accepting the risk of all operational connections to the DISN and all connected systems (DOD Directive 8500.1 (reference e).

j. Connections between DOD, and non-DOD or foreign government information systems will comply with DODI 5200.40 (reference f).

k. Connections between DOD and contractor information systems will comply with DODI 5200.40 (reference f) and DOD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM) (reference n).

l. An inspection/site visit program will support connected systems and enclaves. This program links existing inspection and site assistance/visit actions to support the DISN DAAs accreditation decisions of DISN components and user enclave connections (DOD Instruction 5200.40, reference f, Phase IV).

(1) All enclaves connected to the DISN long-haul are subject to compliance inspections.

(2) All enclaves connected to the DISN long-haul are subject to electronic monitoring for communications management, equipment and enclave configuration compliance assessment and network security purposes.

(3) All electronic monitoring for communications management, equipment and configuration compliance assessment by external organizations will be pre-coordinated with enclave owners.

m. All DOD personnel are personally and individually responsible for providing proper protection of classified information under their custody and control, including information on their information systems and networks. All officials within the DOD who hold command, management (e.g., DAA and Information Assurance Manager (IAM)), or supervisory positions (e.g., Information Assurance Officer (IAO) or supervisors) have specific, responsibility for the implementation and management quality of the Information Security Program within their areas of responsibility (DOD 5200.1-R (reference h)).

n. The DISN will be used for official and authorized purposes only.

(1) This includes emergency communications and any other communications the Combatant Commands determines are necessary in the interest of DOD. In the interest of morale and welfare, Combatant Commanders may approve communications by DOD employees and military members to their family members at home from locations to which they are deployed for extended periods on official business. DISN users will conform to the network policy established by CC/S/A.

(2) Authorized purposes include, for example, brief communications made by military members and DOD employees during official travel to notify family members of transportation or schedule changes. Reasonable personal communications (such as auto or home repair appointments or brief Internet searches) from the military member or DOD employee at his or her workplace are also authorized when the CC/S/A permits categories of such communication and after determining such communications:

(a) Do not adversely affect the DOD organization's performance or military member's or DOD employee's official duties.

(b) Are of reasonable duration and frequency, and whenever possible, made during the employee's or military member's personal time such as after normal duty hours or during lunch periods.

(c) Serve a legitimate public interest, such as enabling DOD employees or military members to stay at their desks rather than requiring them to depart the work area to use commercial systems, or improving the morale of military members and DOD employees stationed away from home for an extended time.

(d) Would not reflect adversely on DOD (e.g., pornography, chain letters, unofficial advertising or soliciting, inappropriate handling of classified information).

(e) Do not overburden the communication system and create no significant additional cost to DOD.

o. DISN non-Defense Satellite Communication System costs will be recovered through the DISA Defense Working Capital Fund through a billing scheme published by DISA. Non-DOD activities will be billed through the respective CC/S/A sponsoring agency.

p. Survivability enhancements in transmission paths, routing, equipment and associated facilities will normally be limited to systems supporting CC/S/A critical missions that justify additional costs.

4. Relationship Between GIG Waiver Board, DSAWG and IA Panel

a. GIG Waiver Board. The purpose of the GIG waiver board is to approve waivers to DISA's Services and DOD policy in such areas as computing services, satellite communications, and NIPRNET/Internet connectivity and information assurance.

b. DSAWG. The DSAWG provides, interprets and approves DISN security policy as authorized under Defense Information System Security Program (DISSP) sponsorship; and develops accreditation approval and/or accreditation recommendations to the four DISN DAAs.

c. Information Assurance Panel (IAP). The IAP, jointly chaired by the Director, Defense Information Assurance Program, and the Chief, Joint Staff, Information Assurance Division, is responsible to the MCEB and the Director, Infrastructure and Information Assurance (I&IA), to act on their behalf to review, develop, coordinate and report recommended DOD positions on IA.

d. Relationships

(1) The IAP serves as the planner level forum to vet, coordinate and synchronize Joint IA issues raised by the DSAWG. The DSAWG

serves as the IAP's subject matter experts for DISN connection approval or certification issues.

(2) DSAWG, as requested, performs analysis on all GIG waiver and appeal requests to determine compliance with all appropriate DISN security policies. Develops recommendations on the acceptability of the waiver/appeal in meeting DISN security policy and whether any DISN security policy waiver should be granted. Provides recommendations to DISA as a part of the assessment of the waiver/appeal and to the GIG Waiver Panel Chair.

e. Figure A-1. Shows the relationship between the GIG Waiver Board, DISN DAA Flag Panel and the Military Communications and Electronics Board (MCEB).

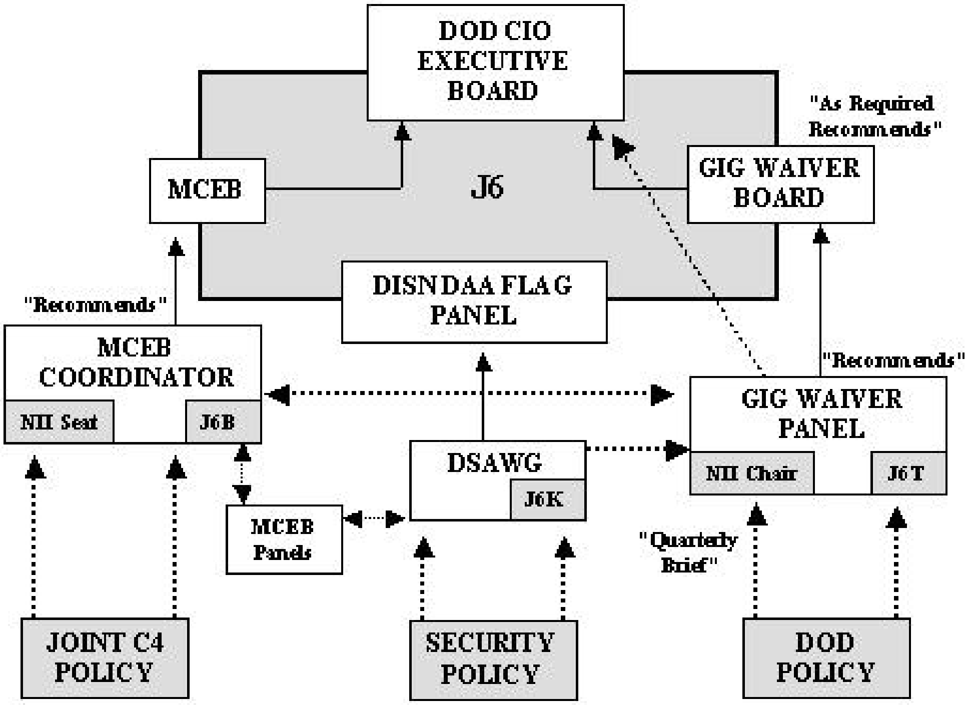

Figure A-1. Relationship Between GIG Waiver Board, DISN DAA and MCEB

ENCLOSURE B

RESPONSIBILITIES

1. Chairman of the Joint Chiefs of Staff (CJCS). The Chairman is responsible for operational network policy and overall direction of the DISN.

a. The Director, Joint Staff, delegates to the Director for Command, Control, Communications and Computer Systems (J-6) authority for operational DISN policy and direction.

b. The Director for Command, Control, Communications, and Computer Systems (J-6), will:

(1) Serve as one of the four DISN DAAs and exercise authority for operational DISN policy and direction.

(2) Appoint a flag-level representative to the DISN Flag Panel.

(3) Appoint an O-6 or civilian equivalent as primary representative to the DSAWG. The Director, J-6, will appoint a primary representative and alternates and identify alternates with Joint Staff DSAWG voting authority. Copy of appointment letter will be provided to DISN Flag Panel and DSAWG chairperson.

(4) Monitor the operational and management effectiveness of the network and report significant items (e.g., major mission degradation) to the CJCS.

(5) Resolve DISN requirement conflicts and issues referred to the Joint Staff or through the MCEB as appropriate.

(6) Develop Joint policy, responsibilities and connection process for DISN. Integrate lessons learned from Information Assurance Panel and DSAWG.

(7) Coordinate assignment of funding responsibility for joint requirements to the appropriate Service.

(8) Validate operational requirement of non-DOD government and contractor connections.

(9) Validate and approve operational requirement of all cross domain connections including combatant command endorsed requests

for foreign entity connections.

(10) Direct joint vulnerability assessment process (JVAP) visits, as required.

(11) Issue disconnection notices as approved by the DISN DAAs.

(12) Establish operational requirement priorities, and prioritize requests for cross domain connections.

2. Combatant Commanders. The combatant commanders in addition to responsibilities in subparagraph 9, will

a. Submit their validated DISN requirements through Service channels, if applicable, to DISA. Commander, US Special Operations Command, will submit requirements directly to OSD.

b. Review and submit service restoration priority requests IAW with DISA Circular 310-130-4 (reference o).

c. Endorse foreign entity connection requests and forward request through the Joint Staff, J-6, for validation and approval.

3. Commander, USSTRATCOM (CDRUSSTRATCOM). CDRUSSTRATCOM in addition to responsibilities in subparagraph 2 and 9 will: Appoint an O-6 or government civilian equivalent as combatant command primary representative to the DSAWG. The USSTRATCOM DAA/Chief Information Officer (CIO) will appoint a primary representative and alternates and identify alternates with USSTRATCOM DSAWG voting authority. Copy of appointment letter will be provided to DISN Flag Panel and DSAWG chairperson.

4. Service Chiefs. The Service Chiefs, in addition to responsibilities in subparagraph 9, will

a. Appoint an O-6 or government civilian equivalent as primary representative to the DSAWG. The Service DAA/CIO will appoint a primary representative and alternates and identify alternates with Service DSAWG voting authority. Copy of appointment letter will be provided to DISN Flag Panel and DSAWG chairperson.

b. Provide local data distribution capability to meet combatant command validated connectivity requirements. (These systems must be focused on supporting operational requirements of the combatant command or parent Service and be capable of supporting contingency operations (e.g., joint task force headquarters)).

c. Appoint a representative to the CDTAB. Formerly known as the SECRET and Below Interoperability (SABI) Process Action Team (PAT).

d. Establish cross domain solution offices to validate and prioritize requests.

e. Coordinate cross domain connections through their Cross Domain Solutions Offices.

f. Provide requisite site support for the DISN equipment located on their respective bases, posts, camps and stations. Support required will include, but is not limited to, providing power, physical security, floor space and on site coordination for the DISN networks points of presence located on their respective bases, posts, camps and stations. Site support will be specified by DISA in appropriate procedural documentation and coordinated with the Service.

5. Director, DISA. The Director, DISA, in addition to responsibilities in subparagraph 9, will:

a. Serve as the DISN network manager.

b. Serve as one of the four DISN DAAs.

c. Appoint a flag-level representative to the DISN Flag Panel.

d. Appoint an O-6 or government civilian equivalent as chairperson of the DSAWG.

e. Appoint an O-6 or government civilian equivalent as primary representative to the DSAWG. The DISA DAA/CIO will appoint a primary representative and alternates and identify alternates with DISA DSAWG voting authority. Copy of appointment letter will be provided to DISN Flag Panel and DSAWG chairperson.

f. Appoint a co-chair person for the CDTAB.

g. Appoint a representative to CDTAB.

h. Assess the technical, programmatic and operational feasibility of adding new services and capabilities to the DISN. New services and capabilities will be added in response to validated user requirements and planned technology insertion.

i. Provide approval for all DISN connections ensuring operational requirements have been validated; connections meet all technical and interoperability requirements; and sub networks, systems and other connected components provide adequate security and have been accredited by the proper authority.

j. Develop, coordinate, and publish DISN connection criteria in conjunction with Services and Defense Agencies.

k. Provide operational management for the DISN and be responsive to the validated operational requirements of the Joint Staff and CC/S/As.

l. Establish a management structure for the DISN and exercise operational direction to include:

(1) Conduct day-to-day network management of the DISN long haul network.

(2) Maintain configuration management of the DISN (e.g., maintaining an accurate and appropriately classified data base of existing DISN user activities, including non-DOD agencies and contractor activities and monitoring system service restoration).

m. Monitor the effectiveness of the DISN-provided services in satisfying user requirements and respond to combatant command requests for reports on system performance.

n. Perform required system engineering and modeling to achieve optimal network design and implementation approach, and identify performance standards for DISN services (e.g., availability and response time).

o. Refer to the Joint Staff any matters that significantly degrade the network.

p. Provide Joint Staff, CC/S/As appropriate periodic status and programmatic updates.

q. Analyze and satisfy requests for new DISN services in coordination with the Joint Staff and appropriate CC/S/As.

r. Specify and maintain the GIG Interconnection Approval Process (GIAP) Web site (http://iase.disa.smil.mil//).

s. Ensure the DISN security architecture meets the needs of the DISN users.

t. Develop and maintain DISN planning and program management process and documentation.

u. Ensure security measures, plans and accreditation policies are based on threat assessments validated by the appropriate member(s) of the DOD community.

v. Provide qualified personnel to conduct compliance assessments of DISN users with connection requirements.

w. Advise the Chairman of the Joint Chiefs of Staff and Commander, USSTRATCOM, on the allocation of DISN resources and network anomalies.

x. Support the combatant commands in creating a network common operational picture (COP) for their area of responsibility (AOR). Maintain field office in support of combatant commands.

y. Coordinate the provisioning of network services across the transport network, IAW CJCS and combatant command requirements. As such, DISA will serve as the single point of contact for CC/S/A DISN managers when they require service continuity across multiple transport networks.

z. Lead technical efforts related to the end-to-end integration and capability of GIG networks to include testing support, interoperability certification and joint spectrum management.

aa. Provide support to the DOD CIO, the Joint Staff, Joint Forces Command, and other combatant commands to achieve GIG network interoperability.

bb. Support NSA development of the overall community cross domain solution architecture.

cc. Establish a cross domain solutions assessment panel (CDSAP) in support of DOD and Intelligence Community (IC) cross domain connection requirements. This panel will approve the expenditure of resources against prioritized requests. An objective of this panel is to deconflict and centralize efforts. Membership will consist of a subset of the DSAWG, Service representatives and others as appropriate.

dd. Establish the SIPRNET Connection Approval Office (SCAO) which will:

(1) Serve as primary coordinator to process and review DOD requests for connection of classified security domains, including, but not limited to the SIPRNET.

(2) Coordinate and manage implementation of cross domain connection requests, and ensure feedback between supporting organizations and the DOD Components.

(3) Track and recommend approval of DOD only, single level connections.

(4) Review implementation of all approved connection requests.

(5) In coordination with NSA, develop and maintain a SIPRNET connection manual describing the step-by-step process the requestor will follow to request and implement a cross domain connection.

(6) Develop and maintain the GIAP-Classified Systems database and web site for recording the technical and operational characteristics of all active connections to include connections between different security domains.

(7) Coordinate with NSA in maintaining SSAA and cross domain appendix (CDA) guidance and templates posted to the GIAP Web site (http://giap.disa.smil.mil//) for use by the customer.

(8) In coordination with NSA, identify vulnerabilities, configuration or operational changes that affect individual or classes of accredited cross domain connection implementations; notify the DSAWG and affected DAAs of such changes.

(9) Ensure through the coordination with enclave DAAs (e.g., base, camp, post or station) that cross domain connection device/requirement are re-certified and re-accredited annually, to include penetration testing, vulnerability and risk assessment, using the risk decision authority criteria. The DISA SCAO will monitor open vulnerabilities to insure compliance.

ee. Provide, in coordination with NSA, semi-annual status reports on cross domain connections (CJCSI 6510.01, reference m) to the DOD CIO, the CJCS and the CC/S/As and their DAAs with active or planned cross domain connections.

ff. Establish the GIAP-Unclassified Systems connection approval office which will:

(1) Serve as the primary coordinator to process and review DOD requests for connection of unclassified domains, including, but not limited to, the NIPRNET.

(2) Coordinate and jointly manage, with OSD, implementation of the customer approval process database for connection requests and ensure feedback between supporting organizations and the DOD components.

(3) Approve requests that are DOD only, single level connections, employing standard equipment configuration conforming to published security configuration guidelines.

(4) Implement all approved connection requests.

(5) Review all commercial Internet waiver requests to DOD systems (network and stand alone).

(6) Develop and maintain a NIPRNET customer connection process guide describing the step-by-step process the requestor will follow to request and implement a NIPRNET or cross domain connection.

(7) Develop and maintain the unclassified systems database and Web site for recording all pending and operational CC/S/A and cross domain connections.

gg. Perform SIPRNET and NIPRNET compliance validation visits to potential high-risk (as identified in Appendix B to Enclosure C) connections. Reports of these visits will be maintained on the DISA/Field Security Office (FSO) Vulnerability Management System (VMS) database.

(1) Reports will be available for review by the DISN DAAs, USSTRATCOM and selective CC/S/As.

(2) Inspected sites can respond to compliance visit open findings via VMS.

(3) Compliance validation visits will consist of traditional security checks, scanning (automated tool) of the connected network and a JVAP

if a device is operational. Download compliance validation visit checklists at web site http://guides.ritchie.disa.mil.

(4) DISA teams will assess the security implementation on the connected environments from the cryptographic device down to the workstation for the SIPRNET connections and from the point of presence of the connection to the servers for the NIPRNET connections.

hh. Where appropriate, operate consolidated cross domain solutions on behalf of the DOD components.

ii. Establish the DISA Cross Domain Implementation Office (CDIO) in support of DOD and IC cross domain connection requirements. The CDIO will:

(1) Coordinate and manage the implementation of cross domain standard solutions, and ensure feedback between supporting organizations and DOD components.

(2) Partner with DOD components to develop a robust cross-domain fielding capability.

(3) Develop and maintain a quick response capability to support immediate wartime fielding teams for cross domain standard solutions.

jj. Establish the CDTAB in coordination with NSA to assess community risks and make recommendations to the DSAWG and DISN DAAs on the connection of implementations to community networks.

kk. Develop, in coordination with NSA, the JVAP to ensure all cross domain connections are assessed on an annual basis.

ll. In coordination with NSA, develop and implement security education, training and awareness program.

mm. Direct and oversee the community evaluation of global risk for networks and their connections in coordination with NSA, DIA and Joint Staff, J-6.

6. Director, DIA. The Director, DIA, in addition to responsibilities in subparagraph 9 will

a. Serve as one of the four DISN DAAs.

b. Appoint a flag-level representative to the DISN Flag Panel.

c. Appoint an O-6 or government civilian equivalent as primary representative to the DSAWG. The DIA DAA/CIO will appoint a primary representative and alternates and identify alternates with DIA DSAWG voting authority. Copy of appointment letter will be provided to DISN Flag Panel and DSAWG chairperson.

d. Implement, operate and manage JWICS components and facilities on the DISN IAW established agreements with DISA.

e. Provide threat data to support the risk assessments and decisions.

7. Director, NSA. The Director, NSA, in addition to responsibilities in subparagraph 9 will

a. Serve as one of the four DISN DAAs.

b. Appoint a flag-level representative to the DISN Flag Panel.

c. Appoint an O-6 or government civilian equivalent primary representative to the DSAWG. The NSA DAA/CIO will appoint a primary representative and alternates and identify alternates with NSA DSAWG voting authority. Copy of appointment letter will be provided to DISN Flag Panel and DSAWG chairperson.

d. Appoint an O-5/GS-14 representative to the CDTAB (co-chair).

e. Provide guidance on required security services and features necessary to meet DISN operational requirements.

f. Recommend techniques and procedures to minimize DISN information security vulnerabilities IAW DODD 8500.1 (reference e) and Chairman of the Joint Chiefs of Staff manual (CJCSM) 6510.01 (reference p).

g. Develop and/or certify communications security (COMSEC) solutions. Produce keying material for all COMSEC.

h. Establish and maintain the methods to perform as well as analyze and evaluate security countermeasures and attacks in support of the community evaluation of the global risk for cross domain solutions.

i. Act as the certification authority for overall cross domain solutions (e.g., guards), not site implementation of the solutions.

j. Establish the NSA Cross Domain Solutions Organization (CDSO) in support of DOD and IC connection requirements, to include:

(1) Develop and maintain (http://iase.disa.smil.mil) the risk decision authority criteria for identifying an acceptable level of community risk appropriate for the connection approval authorities to use in making connection decisions.

(2) Develop the overall community cross domain solution architecture in coordination with DISA and the DOD Service and Agency solution developers.

(3) Develop, maintain and oversee a common DOD and IC process for cross domain solution development, to include specification of robustness and evaluation standards. Referred to as the cross domain solution development process.

(4) Approve the security requirements for cross domain solutions and components and approve the security architecture for cross domain solutions.

(5) Develop and maintain (http://www.iad.nsa.smil.mil) a standard guarding solution listing of recommended, type-certified, connection security implementations. Each standard solution will include guidance for appropriate use including security concept of operations. Oversee community driven improvements to the standard solutions.

(6) In coordination with CC/S/A cross domain solutions organizations and DISA, support site personnel and system developers to adapt existing standard solutions to the specific environment.

(7) Lead the community in the development of new cross domain solutions for requirements not adequately addressed by existing standard solutions. The NSA CDSO will ensure the resulting solution is consistent with the overall cross domain solution architecture.

(8) Identify vulnerabilities that affect individual or classes of accredited connection implementations. Coordinate with DISA on notification of CC/S/As and enclave DAAs for affected systems.

(9) Support DISA development of a SIPRNET connection manual describing the step-by-step process the requestor will follow to request and implement a connection between classified security domains.

(10) Establish a CDTAB in coordination with DISA to assess technical risks and make recommendations to the DSAWG and the DISN DAAs on the connection implementations for community networks.

(11) Provide technical support to DISA for development and conduct of a cross domain JVAP.

(12) In coordination with DISA, develop and implement an education, training and awareness program.

(13) Lead the community in the area of cross domain interoperability, technology and research efforts needed to support future community requirements. Coordinate the activities necessary to ensure a common focus needed for future solution sets.

(14) Designate, in coordination with the community, cross domain solutions as standard solutions.

8. Director, Defense Security Service (DSS). The Director, DSS, administers the National Industrial Security Program (NISP) on behalf of DOD and non-DOD Federal agencies that have entered into an agreement with the Secretary of Defense for the purpose of rendering industrial security services.

9. CC/S/As, DOD Field Activities and Joint Activities will, as applicable

a. Review long-haul common-user transmission requirements and forward all requirements not needing combatant command, the Joint Staff or Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)) validation and approval to DISA for development of technical solution, coordination and implementation.

b. Identify to DISA each DOD system or application device having a requirement for long-haul common-user information transfer services for DISN planning purposes. Systems and requirements will be identified to DISA as soon as requirements for these services are validated.

c. Assess technical, programmatic and operational feasibility of adding new services and capabilities to the DISN in regards to the sustaining base and deployable infrastructure. New services and capabilities will be added in response to validated user requirements and planned technology insertion in coordination with DISA.

d. Coordinate Service and Defense Agency long-haul requirements for DISN access within a combatant commander's geographic AOR, combatant commander/Service/post/camp/station or Agency operated facility and DISA prior to submission.

e. Validate the requirement and maintain oversight for all component connections.

f. Program, budget, fund and provide support for assigned portions of the DISN, including for cross domain connection solution(s) (e.g., guards) development, procurement, training, operation and maintenance as well as usage fees.

g. Deploy standard cross domain solution whenever possible and in conformance with this instruction.

h. Manage DISN sub networks when authorized by the Director, J-6, the Joint Staff, and in conformance with network management policies and procedures issued by DISA.

i. Document and validate the operational and IA requirements for the connection.

j. In conformance with Appendix A (3.b.(2)) prior to initiating any cross domain development or implementation, coordinate with DISA/CDIO and NSA/CDSO. See DOD Instruction 8540.aa (reference l) for additional details.

k. Ensure foreign entity connection requests are endorsed by a combatant command, Service or Agency head and forwarded for validation and approval by the Joint Staff (J-6).

l. Ensure non-DOD (e.g., contractor, other United States Government (USG) agency or organization) connection requests are endorsed (i.e., sponsored) by a DOD organization and forwarded for validation by Joint Staff (J-6) and approval by ASD(NII).

m. Apply applicable information, communications and physical security measures and ensure installation requirements continue to meet the requirements of the DISN security policy.

n. Ensure approved systems use DISN services to meet mission requirements.

o. Ensure user compliance with DISN policy and procedures.

p. Maintain direct management responsibility to coordinate, install, test, and accept their users' host and terminal access circuits according to DISA-established criteria.

q. Provide information, as requested, to DISA for DISN billing, management and inventory purposes.

r. Conduct compliance inspections, assistance visits, technical engineering inspections and remote monitoring and vulnerability assessments of DISN connections and the connected enclaves in support of DISN Information Assurance Program.

s. Establish procedures to ensure prompt and appropriate management action is taken in case of compromise of classified information, or determination that cross domain connections may put classified information at risk of compromise IAW DOD 5200.1-R (reference h).

(1) Actions will focus on correction or elimination of the conditions that caused or occasioned the incident.

(2) Incidents will be reported IAW DOD 5200.1-R (reference h).

(3) Military and civilian personnel will be subject to sanctions if they knowingly, willfully or negligently compromise or put classified information at risk of compromise. Sanctions include, but are not limited to, warning, reprimand, suspension without pay, forfeiture of pay, removal, discharge, loss or denial of access to classified information and removal of classification authority. Action may also be taken under the Uniform Code of Military Justice for violations of that Code and under applicable criminal law.

t. Ensure solution configuration management is maintained.

u. Ensure appointment of enclave DAAs.

10. <u>The Four DISN DAAs, will</u>

a. Serve as the final approval authority for DISN connections and operations after a full evaluation by NSA and DISA of the connection and cross domain technology has been conducted.

b. Appoint DISN Flag Panel members.

c. Delegate in writing approval authority to the Flag Panel, DSAWG and/or DISA SCAO for specific type requests or connections.

d. Assess and manage the risk of operating all connected systems within the DISN.

e. Serve as the approving authority for all DOD classified cross domain solutions.

f. Serve as the final appeal for connection requests. Unanimous approval by DISN DAAs required for connection.

g. Make final determination, with DSAWG and Flag Panel recommendation, to disconnect or disapprove a cross domain connection or cross domain solution (see figure C-4).

h. Annually review cross domain connections. Because these connections are considered high risk, they will be re-accredited annually, and re-certification of the connection will include a JVAP.

i. Validate the operational requirement for all connections between different security domains prior to engineering the interconnection solution.

11. <u>DISN Flag Panel will</u>

a. Support the DISN DAAs in their role as final approval authority for all DISN connections and cross domain solutions, and in their annual review of operational connections.

b. Make connection approval recommendations to the DISN DAAs, and make connection approval decisions for those classes of systems and circumstances delegated by the DISN DAAs.

c. Review and approve DSAWG responsibilities and membership.

d. Review and adjudicate DSAWG recommendation(s) on connections involving new technology, high risk or foreign nationals and make recommendations to the DISN DAAs for the disconnection or disapproval of a cross domain solution.

e. Review appeals from connection sponsors of DSAWG decisions. Support the DISN DAAs in their annual review of operational connections.

12. DISN Security Accreditation Working Group (DSAWG) will

a. Support DISN DAA's in their role as final approval authority for all DISN connections.

b. Make connection approval recommendations to the Flag Panel and DISN DAA's.

c. Make connection approval decisions for those classes of systems and circumstances delegated by the DISN DAAs (e.g., similar architectures and cross domain systems previously approved by DISN DAAs).

d. Make recommendations to the Flag Panel and DISN DAAs for the disconnection or disapproval of a cross domain solution.

e. Develop and coordinate the approval of the DISN Security Policy.

f. Guide or assist development of DISN integrated system/security architecture and policy changes.

g. Provide the DOD community risk assessment for all cross domain connections between classified domains including, but not limited to, connections to the DISN.

h. Provide early assessment of risk to the DISN Flag Panel.

i. Coordinate with the Defense and Intelligence Community Accreditation Support Team (DICAST) and the IC Information Assurance Policy Board (IAPB) on all cross domain connections between TOP SECRET/Sensitive Compartmented Information (SCI) and other DOD classified domains including, but not limited to, connections to the DISN.

j. Monitor life cycle of the DISN long-haul service to identify and resolve security issues.

k. Make DISN connection accreditation policy recommendations to the MCEB.

l. Make recommendations to the DISN Flag Panel on resource prioritization for DISN connection requests.

m. Provide security assessments to the GIG Waiver Review Panel in support of the DOD CIO GIG Waiver Process. Note: The GIG Waiver Review Panel supports the DOD CIO Executive Board for Requests for Waiver of the DISN.

13. The Cross Domain Technical Advisory Board (CDTAB) will

a. Act as an advisory board to the DSAWG.

b. Perform technical risk assessments of cross domain solutions.

c. Report results of the assessments (and possible alternative proposals to mitigate risk) to the DSAWG.

d. Operate under the direct guidance of the DSAWG and the general guidance of the Flag Panel.

e. Be co-chaired by DISA and NSA.

14. Enclave DAAs will execute the following responsibilities for connection to DISN

a. Ensure compliance with the GIAP process.

b. Identify and inform other DAAs affected by the connection and assist in developing the associated community risk assessment.

c. Ensure local risk assessment of each connection implementation is conducted to determine whether the local level of risk is acceptable. Develop and implement the SSAA to maintain configuration control of the connection.

d. Ensure that the user network is re-accredited every 3 years or when network meets re-certification conditions described in DOD Instruction 5200.40 (reference f). Re-accreditation should include penetration testing, vulnerability and risk assessment and configuration compliance review.

e. Review of all cross domain connections annually to ensure valid operational requirement still exists, the current implementation satisfies the requirement and the SCAO has been notified of the continuing requirement.

f. Ensure connected enclaves with cross domain solutions are certified and accredited annually.

g. Ensure a properly conducted certification is accomplished on each system considered for accreditation IAW DITSCAP.

h. Grant final and interim accreditation of a network or system entirely under their control.

i. Verify that each SSAA complies with information system security requirements as reported by the IAM. Ensure the operational information systems security policies are in place for each system, project, program and organization or site for which the DAA has approval authority.

j. Ensure records are maintained for all existing information system accreditations or certifications under the DAA's purview.

k. Request DSAWG approval for additional security mechanisms and software (e.g., encryption and guards) necessary for DISN connection and comply with connection procedures.

l. Ensure, when classified or sensitive information is exchanged between logically connected components at the same classification level, the content of this communication is protected from unauthorized observation by acceptable means, such as encryption or protected distribution systems (PDS) (see National Security Telecommunications and Information Systems Security Instruction (NSTISSI 7003, reference q).

m. Validate the operational and functional requirements for all cross domain connection requests.

n. Validate the implementation-independent information protection requirements with other affected enclave DAAs as appropriate.

o. Submit and maintain current information on connection requests through the SCAO Web site.

p. Develop and maintain the CDA to maintain configuration control of the connection implementation.

q. Maintain configuration management descriptions of the site/enclave and all communications that enter/egress the site/enclave.

15. Information Assurance Manager (IAM). The IAM will carry out responsibilities outlined in CJCSM 6510.01 (reference p). Note: The term IAM may be used interchangeably with the IA title Information Systems Security Manager (ISSM).

16. Information Assurance Officer (IAO). The IAO will carry out responsibilities outlined in CJCSM 6510.01 (reference p) and support the JVAP. Note: The term IAO may be used interchangeably with other IA titles (e.g., Information Systems Security Officer (ISSO), Information Systems Security Custodian, Network Security Officer, or Terminal Area Security Officer).

17. Program Manager. The Program Manager for multi-site/multi user application or system will identify security features for centrally developed systems. Such features will be documented IAW DOD Instruction 5200.40 (reference f) and briefed to the DSAWG for approval/validation before undertaking development and before fielding. Ports and protocol compliance will be specifically addressed. To minimize the impact on multiple sites attempting to conduct separate, security relevant testing, the developers are expected to accomplish as much of this testing and related documentation prior to full scale fielding. Developer will comply with DOD Instruction 5200.40 (reference f) in developing such security relevant documentation. Selected versions or configurations will be developed, documented and sufficiently tested to minimize the unique testing to be accomplished at each site. The developer will provide site sufficient documentation to permit the site DAA to verify security aspects of any site unique configuration features or settings (hardware or software). This process is known as type accreditation (see NIST Special Publication 800-37, reference r).

18. Cross Domain Solution Program Manager (CDSPM). The CDSPM will maintain life-cycle configuration.

ENCLOSURE C

CONNECTION PROCESS

1. Connection Process. Connection processes are written from the perspective of a site initiating the request. Services and Agencies may centrally develop specific technology that will be fielded to multiple sites (paragraph 17, Enclosure B). In such cases, those program offices will follow this process to achieve type accreditation status of the security features of the technology/system (e.g., port and protocol compliance or cross domain technology).

2. Appendix A. Provides guidance on SIPRNET connection requests to include cross domain interfaces.

3. Appendix B. Provides guidance on unclassified DISN connection requests.

4. Appendix C. Provides guidance on DVS connection requests.

5. Appendix D. Provides guidance on validation and approval request for DOD cross domain, non-government, contractor or foreign entity connections.

6. Appendix E. Provides guidance on DISN Information Assurance Program, which is the sustaining effort to validate enclave compliance with connection requirements.

7. JWICS Connection Requests

a. JWICS connection requests are the responsibility of DIA.

b. The connection process for JWICS is documented in the "JWICS Connection Policy, " which can be found at www.jwics.ic.gov.

8. Interim Certification To Operate (ICTO) Requests

a. Authority to field new systems or capabilities for a limited time, with a limited number of platforms to support developmental efforts, demonstrations, exercises, or operational use requires an ICTO. The decision to grant an ICTO will be made by the Interoperability Policy and Test Panel (IPTP) (sub-panel of the MCEB) based on the sponsoring component's initial laboratory test results and the assessed impact, if any, on the operational networks to be employed.

b. An ICTO is appropriate only in exceptional cases where a system cannot complete Interoperability Certification testing requirements prior to fielding for the following reasons:

(1) Urgent operational needs requiring fielding prior to testing.

(2) The first system to implement an interface.

(3) Similar situations that may warrant the granting of an ICTO and are approved by the IPTP.

c. An ICTO is not appropriate for systems that have completed Interoperability Testing and failed to meet the identified interoperability requirements. The decision to field a system is the responsibility of the specific system fielding authority and should consider either the ICTO or the interoperability certification letter/test report in making that decision.

d. An ICTO shall not exceed 1 year in duration. Extensions may be considered by the IPTP.

APPENDIX A TO ENCLOSURE C

SIPRNET CONNECTION REQUESTS

1. General

a. SIPRNET (as a transport application) is operated in the SECRET US Only System High mode. Enclaves may process information with various handling or access restrictions. No directly connected enclave will process information classified higher than SECRET.

b. All enclaves must complete the requirements in paragraph 2 that represents basic connection documentation requirements. This includes enclaves that process information at classifications other than US SECRET. Such connections will be made via approved cryptographic solutions.

c. Enclaves that host solutions to receive information from other enclaves in different security domains will follow the process in paragraph 3.

d. Connection Request uses language from the perspective of a site initiating the request. While sites will always be the ultimate location of this technology development work, prior to fielding to multiple sites, this development work may be accomplished via Service and Agency program efforts. In such cases, in compliance with DOD Instruction 5200.40 (reference f), those program offices will follow this process to achieve type accreditation status if their product relies upon cross-domain technology.

2. SIPRNET Connection Approval Office (SCAO) SIPRNET Connection Approval Process (SIPRCAP) (Figure C-A-1)

a. Pre-Connection Requirements - In preparation for connection the organization having connection requirement will:

(1) Determine and document the mission needs the connection will support.

(a) Contact the SIPRNET Program Management Office and submit Initial Modeling Request (IMR) for connection access to the SIPRNET.

(b) For government non-DOD activities the DOD sponsor has to submit a request for validation of the connection requirement to the Joint Staff (J6). (Figure C-A-2)

(c) For contractor activities the DOD sponsor has to submit a request for validation of the connection requirement to the Joint Staff (J6) and notify the DSS Program Management Office of possible future classified connection requirements at the contractor facility. (Figure C-A-2)

(2) Submit Request for Service (RFS) to the servicing Telecommunication Certification Office (TCO) to begin the connection process.

b. Connection Requirements – Requirements for connection can be found on the DISA IA Web site (HTTPS://iase.disa.mil/CAP/capsiprnet.html//), SIPRCAP page. If the connection includes any transfer of information between different classification domains (i.e., classified to unclassified, classified SECRET to coalition, etc), reference the SCAO Cross Domain Interface Process (CDIP) paragraph 3. below.

(1) Interim Approval to Connect (IATC). The IATC defines the customer's connection boundaries as accepted by the DISN SIPRNET Management. The minimum requirements for connection include (reference the SIPRCAP page of the DISA IA Web site):

(a) Interim Authority to Operate (IATO). The IATO documents the local DAA's acceptance of the risk for operations and defines the enclave accreditation boundaries in accordance with applicable CC/S/A directives.

(b) Consent to Monitor (CTM). The CTM is the local DAA's declaration to allow DISA to access to assess their network infrastructure.

(c) SIPRNET Access Assessment Questionnaire (SAA). The SAA provides specific local network information.

(d) Network Diagram. The network topology reflects all of the devices that are connected logical/physically to the local classified infrastructure.

(2) Authority to Connect (ATC). The ATC defines the customer's connection boundaries as accepted by the DISN SIPRNET Management

and reflects the completion of a successful network vulnerability assessment by the DISA SCAO. The requirements for an ATC include (reference the SIPRCAP page of the DISA IA Web site):

(a) System Security Authorization Agreement (SSAA). A copy of the enclave SSAA is required to complete the documentation required for connection to the SIPRNET (DOD Instruction 5200.40, reference f).

(b) Consent to Monitor (CTM). The CTM is the local DAA's declaration to allow DISA to access to assess their network infrastructure.

(c) SIPRNET Access Assessment Questionnaire (SAA). The SAA provides specific local network information.

(d) Network Compliance Assessment. The network must have successfully completed compliance and vulnerability Assessment performed by the SIPRNET, SCAO.

c. Connection Termination

(1) SCAO will

(a) Inform the DISN Flag Panel via the DSAWG of site non-compliance.

(b) Notify the site and the appropriate CC/S/A representative.

(c) Continue contact with the site to monitor remedial actions. If actions are unsatisfactory, the SCAO will advise the J6, Joint Staff.

(2) Flag Panel will: Recommend to Joint Staff/J6 that a disconnect notice be issued.

(3) Joint Staff, J-6 will

(a) Initiate coordination with J3 and enclave component to assess operational impact of potential disconnects.

(b) Release a message giving 30 days to bring the connection into compliance or submit a plan to achieve connection compliance. Submitted plan must lead to compliance within 60 days of notification message release.

(c) Issue a coordinated DISN DAA order to disconnect, if compliance is not achieved within 30 day or 60 day windows.

(4) DISA Network Operations will: Verify and implement disconnection as directed.

(5) Site DAA will: Terminate connection as directed by the DISN DAA's, notify the SCAO via routine letter/message and submit appropriate disconnection request (RFS through their TCO).

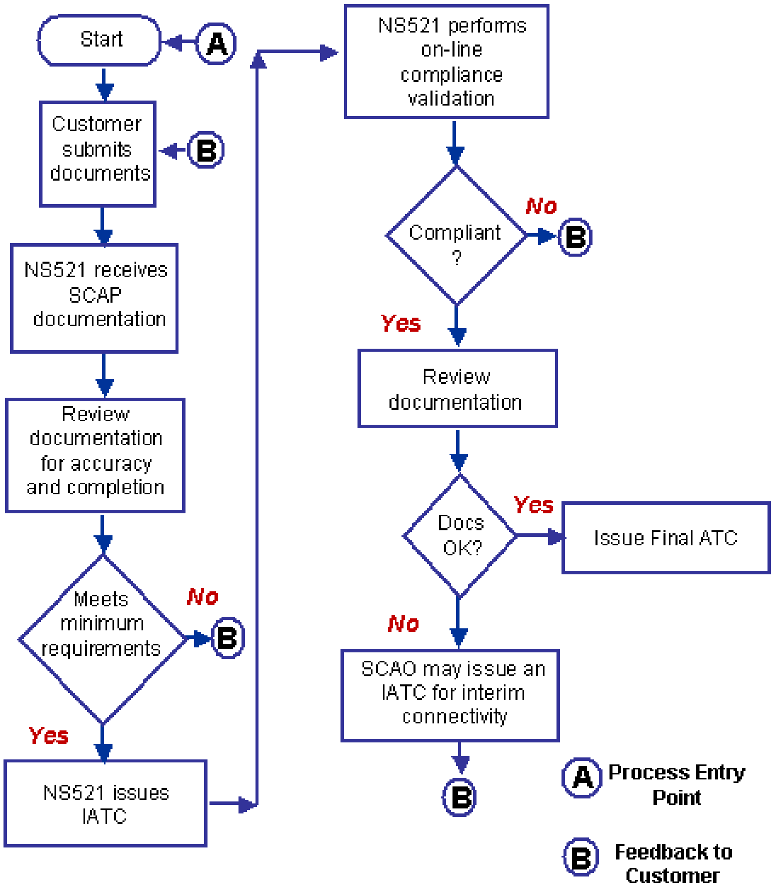
Start
A
Customer submits documents
B
NS521 receives SCAP documentation
Review documentation for accuracy and completion
Meets minimum requirements
No
B
Yes
NS521 issues IATC
NS521 performs on-line compliance validation
Compliant ?
No
B
Yes
Review documentation
Docs OK?
Yes
Issue Final ATC
No
SCAO may issue an IATC for interim connectivity
B
A Process Entry Point
B Feedback to Customer

Figure C-A-1. Conventional Connection

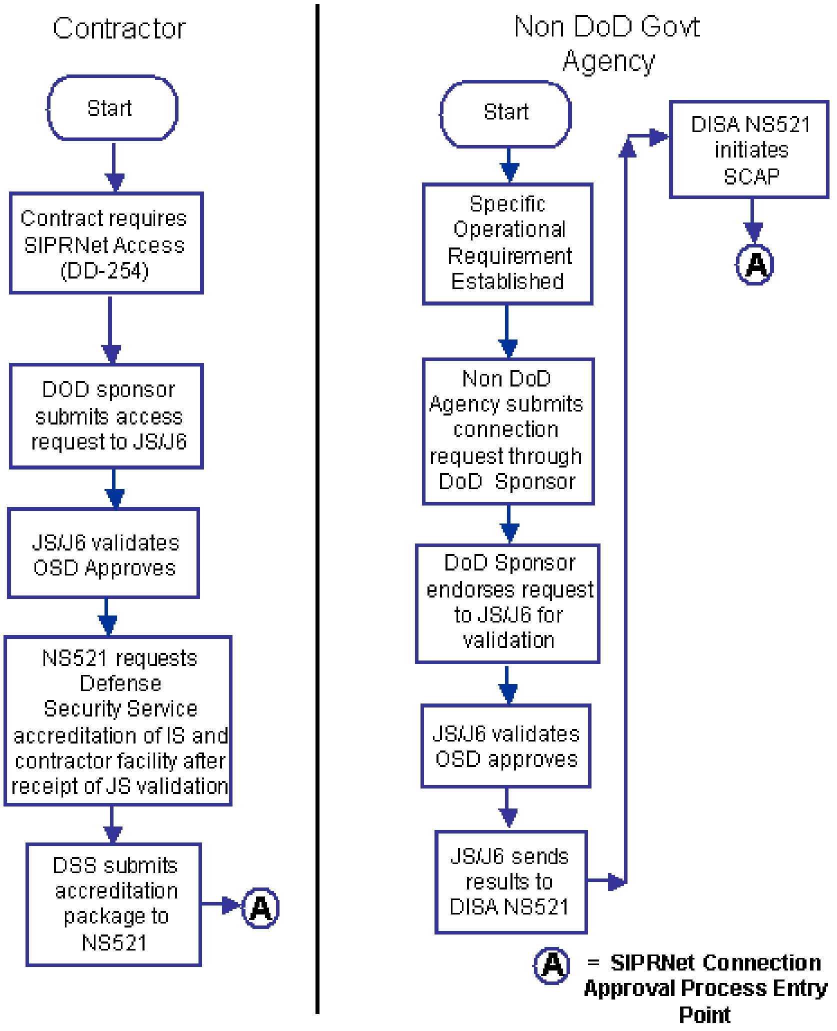
Contractor
Start
Contract requires SIPRNet Access (DD-254)
DOD sponsor submits access request to JS/J6
JS/J6 validates OSD Approves
NS521 requests Defense Security Service accreditation of IS and contractor facility after receipt of JS validation
DSS submits accreditation package to NS521
A
Non DoD Govt Agency
Start
Specific Operational Requirement Established
Non DoD Agency submits connection request through DoD Sponsor
DoD Sponsor endorses request to JS/J6 for validation
JS/J6 validates OSD approves
JS/J6 sends results to DISA NS521
DISA NS521 initiates SCAP
A
A = SIPRNet Connection Approval Process Entry Point

Figure C-A-2. Contractor and Non-DOD Government SIPRNET Access

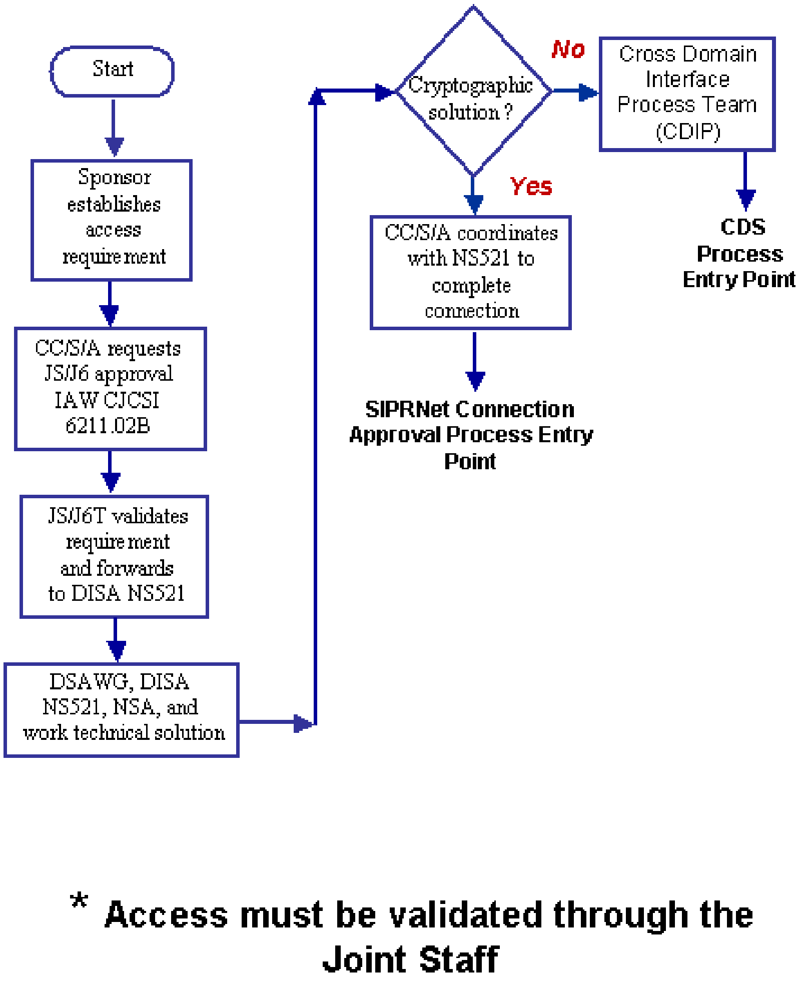
Start
Sponsor establishes access requirement
CC/S/A requests JS/J6 approval IAW CJCSI 6211.02B
JS/J6T validates requirement and forwards to DISA NS521
DSAWG, DISA NS521, NSA, and work technical solution
Cryptographic solution ?
No
Cross Domain Interface Process Team (CDIP)
CDS Process Entry Point
Yes
CC/S/A coordinates with NS521 to complete connection
SIPRNet Connection Approval Process Entry Point
* Access must be validated through the Joint Staff

Figure C-A-3. Foreign Network Access

3. Cross Domain Interface Process (CDIP) (Figure C-4)

a. Step 0: Prepare Request

(1) In preparation for connection registration, organization having connection requirement will:

(a) Determine and document the mission needs the connection will support. These operational requirements will be validated.

(b) Document the implementation information protection requirements and have the protection requirements validated. CC/S/As solution providers may assist in the documentation of protection requirements. Implementation information protection requirements will include:

1 Information types and classifications.

2 Type of user access required.

3 Applicable policy.

4 Characterization of threats to the information types and classifications (types and characterization of adversaries, adversary attack types and motivations).

5 Required security services and strengths.

(c) DAAs representing the enclaves to be connected will validate the implementation-independent information protection requirements. The Enclave DAA will:

1 Validate the protection requirements for the connected domains, if the security domains to be connected are under a single or multiple involved DAAs with no DISN managed connectivity.

2 Validate the protection requirements for his domain.

3 Ensure there is a valid operational requirement for all connections.

(d) DISN DAAs will: Validate the protection requirements for the interconnected community, if the security domains to be connected involve any DISN managed connectivity.

b. Step 1 – Authorize and Prioritize Request

(1) Requests for single-level SIPRNET connection for DOD organizations are validated by requesting DAA and submitted to the SCAO.

(2) Requests for cross domain connection requirements of US classified or unclassified enclaves/networks to the DISN must be:

(a) Endorsed by the appropriate CC/S/A headquarters.

(b) Validated and approved IAW Appendix D prior to or simultaneously with submitting connection requirement.

(3) Requests for cross domain solution connected to the DISN for DOD organizations, non-DOD US government organizations, contractors and foreign entities (Figure C-A-3) must be:

(a) Endorsed by the appropriate CC/S/A headquarters.

(b) Validated and approved IAW Appendix D prior to or simultaneously with submitting connection requirement.

(4) CC/S/A will: Validate and prioritize their cross domain connection requests and update prioritization whenever new requests are submitted.

(5) For a cross domain connection the Service CDSO will

(a) Authorize and prioritize request.

(b) Make an initial recommendation on whether a standard solution from the standard guarding solutions list can be used or a new solution must be developed.

(c) Forward the request to the DISA Registration and Triage Team for a standard solution, or to the NSA Registration and Triage Team for a new solution.

c. Step 2: Process Request

(1) DAA Requesting Connection of Enclaves will: Submit connection request through the SCAO for single level connections. Cross domain connections requests are submitted through the Service CDSO.

(2) For conventional (single level) connection, DISA SCAO will:

(a) Ensure appropriate validation of each request.

(b) Validate type of connection request.

(c) Assign ticket number and track requests throughout process.

(d) Forward request to SIPRNET Connection Approval Process (SIPRCAP) for connection.

(e) Determine the accreditation status of the enclaves before certifying the connection.

(f) Upon completion of SIPRCAP, proceed to Step 5: Connection Approval.

(3) <u>For a cross domain connection, the Registration and Triage Team will</u>

(a) Validate whether a standard solution is to be used or a new solution is to be developed.

(b) Perform an initial risk overview of the request.

(c) Determine whether or not DISN connectivity is involved.

(d) Enter the request into the SCAO database.

(e) Forward the request package to the CDSAP for approval to apply resources.

d. <u>Step 3: Community Approval</u>. For cross domain connections requests only. The CDSAP will

(1) Review connection request package.

(2) Prioritize request.

(3) Determine whether or not resources should be applied.

(4) For a standard solution, forward request to DISA for implementation. For a new solution, forward request to NSA for development.

e. Step 4: Develop/Implement Connection Solution (Cross domain connections only)

(1) For standard implementation, DISA will:

(a) Work with the site point of contact (POC) and appropriate CC/S/A solution provider to adopt standard solution to the specific requirement.

(b) Ensure the resulting solution is consistent with the overall community cross domain architecture.

(c) Approve the engineering documentation and implementation of the adapted solution.

(d) Facilitate the community security evaluation organizations (e.g., DISA, NSA and DIA) in performing security evaluations and risk assessments of cross domain solutions.

(2) For new solution development NSA CDSO will

(a) Work with the site POC, the DISA SCAO and appropriate C/S/A developers to engineer a new solution.

(b) Lead the security engineering effort to

1 Ensure the resulting solution is consistent with the overall community cross domain architecture.

2 Approve the development of new cross domain components.

3 Approve security requirements and security architecture.

4 Ensure the organization security evaluation criteria reflect the desired security functions and attributes.

(c) CDTAB will perform security evaluations and risk assessments of the cross domain solutions, in coordination with the NSA CDSO and present to the DSAWG, Flag Panel, DAAs for approval to implement at the site.

(d) Work with site POC, and appropriate CC/S/A developers to implement the new solution at the site.

(e) Cross Domain Technical Advisory Board (CDTAB) will

1 Review security evaluations and risk assessments.

2 Forward connection recommendations to the appropriate approval body (DSAWG, Flag Panel and DISN DAAs) through the DISA SCAO.

f. Step 5: Connection Approval

(1) DISA SCAO will

(a) Review the entire request and other related documentation and provide guidance to the connection approval authorities.

(b) Document the accreditation status of the enclave on both sides of the connection.

(2) Single DAA will: Accredit the connection and notify the DISA SCAO, if the security domains of the interconnected systems are under a single DAA with no DISN connectivity.

(3) Multiple Involved DAAs will: Accredit the connection and notify the DISA SCAO, if the security domains involve more than one DAA but no DISN managed connectivity.

(4) DISN DAAs will

(a) Approve the connection of the enclave to the long-haul transport infrastructure, if the security domains involve DISN managed connectivity. The enclave DAA accredits the enclave being connected.

(b) Delegate authority to the Flag Panel, DSAWG or DISA SCAO for some connection decisions. The DISN DAAs remain the decision authority for those connections not delegated.

(5) DSAWG will: Review and approve cross domain solution connections (as delegated) or forward recommendation(s) to the Flag Panel.

(6) Flag Panel will: Review and approve cross domain solution connections (as delegated) or forward recommendation(s) to DISN DAAs for final resolution.

g. Step 6: Connection

(1) DISN DAAs, Flag Panel or DSAWG will: provide connection approval or disapproval recommendations to the DISA SCAO.

(2) DISA SCAO will

(a) Notify the site and CC/S/A DAA of the decision, results and conditions (including time limits) an ATC letter.

(b) Ensure enclave package is complete.

(c) Grant connection approval.

(d) Notify the site and appropriate CC/S/A DAA of disapproval.

(3) Enclave DAAs will: Operate the approved enclave connection in compliance with approved conditions provided by DISA SCAO via ATC letter.

(4) DSAWG will

(a) Review cross domain connections semi-annually to ensure a valid operational requirement for the connection still exists and the current implementation satisfies the requirement.

(b) Re-accredit connections considered high risk annually. Re-accreditation of the high-risk connections will include a JVAP. On-site JVAP is conducted annually, or as directed by the Joint Staff.

h. Step 6A: Disconnection

(1) DISA SCAO will

(a) Inform the DISN Flag Panel via the DSAWG of site non-compliance.

(b) Notify the site and the appropriate CC/S/A representative.

(c) Continue contact with the site to monitor remedial actions. If actions are unsatisfactory, the DISA SCAO advises the Joint Staff, J-6.

(2) Flag Panel will: Recommend to Joint Staff, J6 that a disconnect notice be issued.

(3) Joint Staff (J-6/J-3) will

(a) Initiate coordination with enclave component to assess operational impact of the potential disconnects.

(b) Release a message giving 30 days to bring the connection into compliance or submit a plan to achieve connection compliance. Submitted plan must lead to compliance within 60 days of notification message release.

(c) Issue a coordinated DISN DAA order to disconnect, if compliance is not achieved within 30 day or 60 day windows.

(4) DISA Network Operations will: Verify and implement disconnection as directed.

(5) Enclave DAA will

(a) Disconnect device with approval from their senior headquarters, if DAA determines any device in the enclave, including cross domain solution, is no longer required. The DAA will notify the DISA SCAO via letter and update the site SSAA and SAA.

(b) Terminate connection, if DAA determines that a connection is no longer required, notify the DISA SCAO via routine letter/message and submit appropriate disconnection request (RFS through TCO).

4. Timelines for Cross Domain SIPRNET Connection Requirements

a. Joint Staff, J-6, and ASD(NII) will

(1) Validate and approve operational requirement for DOD and foreign cross domain connection requests within 5 working days, if all required information is provided by requesting/endorsing DOD organization.

(2) Validate operational requirement for non-DOD government and contractor and foreign cross domain connection requests. ASD(NII) will

approve non-DOD government and contractor cross domain connection requests. Validation and approval will be completed within 5 working days, if all required information is provided by requesting/endorsing DOD organization.

(3) Validate and approve operational requirement for "CRITICAL" connection requests can be completed in 24 hours, if all required information is provided by requesting/endorsing DOD organization.

b. DISA SCAO will assign tracking number within 2 working days.

c. DISA will complete engineering and evaluation within 10-12 weeks for connection requirements requiring only tailoring of standard solutions. Actual timelines for completion will depend on completeness of information provided, overall priorities, extent of tailoring required and existence of any significant funding issues. Note: Use or tailoring of an approved cross domain solution will reduce potential engineering and evaluation timelines and effort required.

d. NSA will complete engineering and evaluation within 52-78 weeks for connection requirements requiring development of new cross domain solution. Actual timelines for completion will depend on completeness of information provided, complexity of the proposed new solution, overall priorities, and funding. Note: This is least preferred solution for time-sensitive requirements due to potential engineering and evaluation effort required and unforeseen technical problems.

e. DSAWG, Flag Panel and DISN DAA will: Approve connection within 1-3 weeks depending on level of approval required (DSAWG, Flag Panel, or DISN DAAs), completion of engineering and evaluation steps and time sensitivity of request. Note: Approval process coordination can be run concurrently for high priority (time sensitive) connection requirements, but engineering and evaluation steps must still be completed prior to final approval.

5. Point of Contact: The SCAO (scao@ncr.disa.mil or scao@ncr.disa.smil.mil) serves as the single POC for SIPRNET connections.

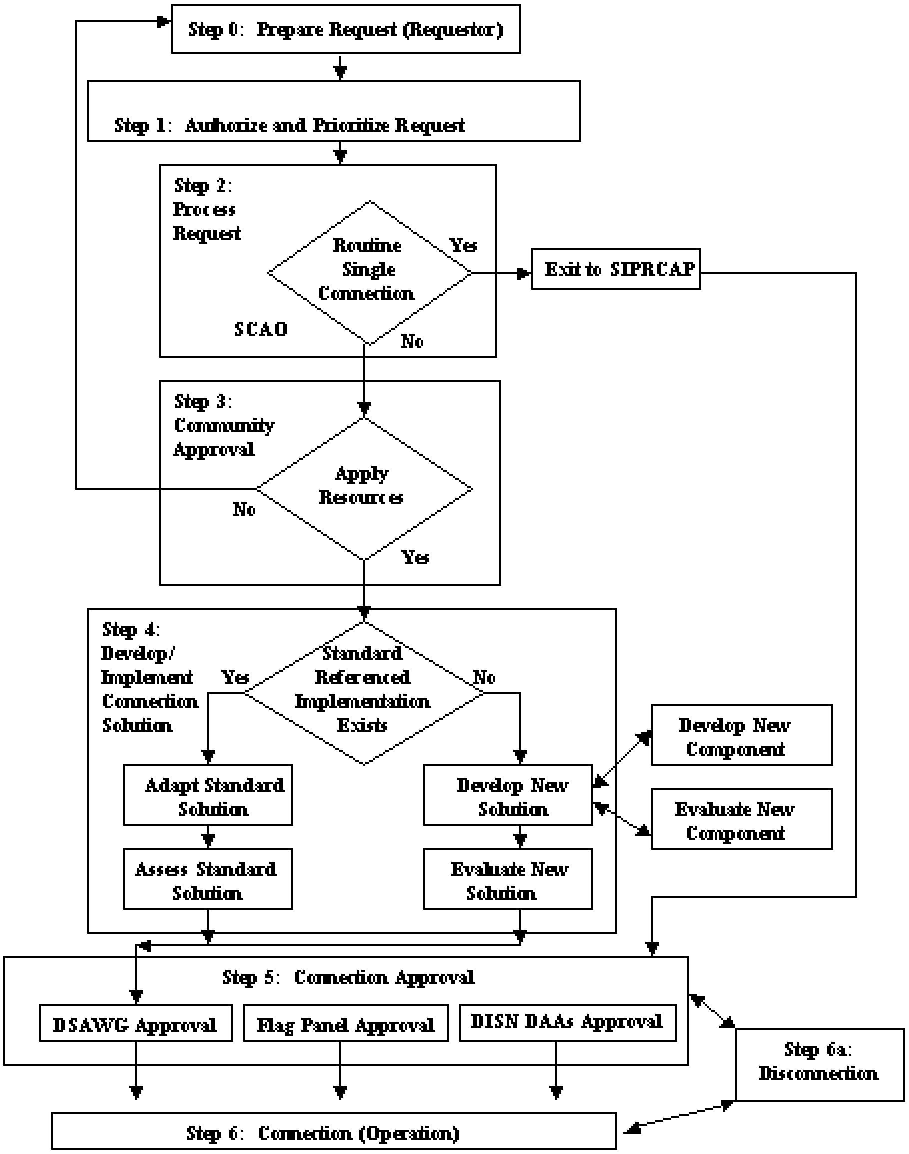

Figure C-A-4. Connection Process (SIPRNET)

(INTENTIONALLY BLANK)

APPENDIX B TO ENCLOSURE C

NIPRNET CONNECTION REQUESTS

1. Unclassified DISN Connection Approval Requests

a Step 0: Prepare Request. CC/S/A review connection requirement and prepare information for completing Unclassified DISN connection approval request or waiver. See Connection Approval Process (CAP) electronic form on System/Network Approval Process Web site for more information required (HTTPS://cap.nipr.mil//).

b Step 1: Registration and Use of DISN Connection Approval Requirements.

(1) Requesting Organization will register Unclassified DISN connection, by completing the CAP online form, which is submitted electronically via the System/Network Approval Process Web site (HTTPS://cap.nipr.mil//).

(2) System/Network Approval Process Manager will

(a) Ensure appropriate validation of each non-DOD request.

(b) Determine type of connection request. Connection types:

1 Conventional connection. If the connection is a routine connection move directly to step 2.

2 Commercial ISP connection. If commercial Internet Service Provider (ISP) connection is required, see paragraph 2.

c. Step 2: Connection Approval

(1) Conventional connection.

(a) System/Network Approval Process Manager will

1 Notify the requesting organization/user about its approval to connect to the unclassified DISN.

2 Send organization a Registration Tracking number and Consent to Monitor form. The Registration Tracking number is necessary for you to make any future changes or updates to the CAP

database.

(b) Requesting organization will

1 Sign the Consent to Monitor form (must be signed by the organization's commander, DAA, or other command-designated official).

2 Fax the Consent to Monitor form to (703) 882-2885 or mail signed form to:

DISA, NIPRNET CAP (NS52)
5275 Leesburg Pike
Falls Church, VA 22041

d. Step 3 Unclassified DISN Disconnect

(1) System/Network Approval Process Manager will

(a) Determine if a site is non-compliant.

(b) Notify the site and appropriate CC/S/A representative.

(c) Continue contact with the site to monitor remedial actions. If actions are unsatisfactory, the NIPRNET Connection Approval Office (NCAO) informs the DISN Flag Panel via the DSAWG of site non-compliance.

(2) Flag Panel will recommend to the Joint Staff, J-6, that a disconnect warning notice be issued.

(3) Joint Staff will

(a) Initiate coordination with J-3 and enclave component to assess operational impact of the potential disconnects.

(b) Release a message giving 30 days to bring the connection into compliance or submit a plan to achieve connection compliance. Submitted plan must lead to compliance within 60 days of notification message release.

(c) Issue a coordinated DISN DAA order to disconnect, if compliance is not achieved within 30 day or 60 day windows.

(4) Enclave DAA. Will within 30 days bring the connection into compliance release, or submit appropriate Request for Service (RFS) to their Telecommunications Control Officer to disconnect service.

(5) DISA network operators. Verify and implement disconnection as directed.

2. Internet Waiver/User Enclave Waiver Process

a. Step 1: Register a NIPRNET to Internet Waiver/User Enclave Waiver. An Internet waiver is required for temporary approval for a CC/S/A to connect to Internet and the DISN. A User Enclave Waiver is required for a connection to the Internet by a CC/S/A that is not connected to the unclassified DISN. Consideration will be based on compliance with DOD IA and CND policies.

(1) Requesting organization will complete the NIPRNET to Internet Waiver/User Enclave Waiver form, which is submitted electronically via the NIPRNET CAP Web site.

(2) DOD Component CIO

(a) Review waiver request for compliance to DOD GIG policy, DISN capability, and technical security requirements.

(b) Coordinate schedule and presentations with the System/Network Approval Process Program Manager, DSAWG and OSD GIG Waiver Panel.

(c) Resolve concerns and questions as directed by the Information Assurance waiver.

(3) System/Network Approval Process Manager will

(a) Review entire request and other related documentation and provide guidance to the connection approval authorities.

(b) Evaluate the data for completeness and DOD IA and CND compliance.

b. Evaluation of the Waiver Connection Implementation

(1) System/Network Approval Process Manager will: Determine if organization security devices and procedures meet DOD security

controls/requirements.

(2) DISN Accreditation review authorities (e.g., DSAWG, Flag Panel) will: Perform a technical review of the IA Compliance Assessment of the waiver and make a recommendation to the appropriate reviewing body.

(3) OSD GIG Waiver Panel will: Review all assessments from DISA, DISN Accreditation review authorities, and other IA technical review activities before making a recommendation to the DOD CIO.

c. Step 2: Disconnection. See paragraph 1.d. above.

3. Points of contacts: Contact the System/Network Approval Process Support Center at capnipr@ncr.disa.mil or calling (703) 882-2086.

APPENDIX C TO ENCLOSURE C

DISN VIDEO SERVICES (DVS) CONNECTION REQUESTS

1. Background.

a. DISN Video Services (DVS). DVS is the video transfer portion of the DISN. It supports controlled, UNCLASSIFIED through TOP SECRET video teleconferences, on a worldwide basis. The connection requirements defined below must be met before teleconferences are allowed.

b. The major components of the DVS connection process are

(1) Database to manage and provide status information on the approval process.

(2) Objective evaluation of customer documentation to determine if customer documentation meets security criteria.

(3) System verification testing activity.

2. DVS Registration Process. DVS customer sites must be registered with DISN Video Services.

a. Step 1: Initial Contact. Customers desiring connection to DVS must contact the appropriate DVS Account Manager (AM). Identification and telephone number of the AM assigned to each CC/S/A can be obtained by contacting DISN's Video Services Division, NS55 at DSN 312-381-1939 or COML 703-882-1939. Customers may also visit the web page at http://disa.dtic.mil/disn/vtc (Becoming a customer).

b. Step 2: DVS System Security Package

(1) Each customer requiring video services connectivity must submit an Approval to Operate (ATO) or IATO letter from the cognizant DAA to the appropriate DISA AM.

(a) ATO Letter

1. Each ATO letter must identify mode(s) of operation; highest classification level of information being processed; and any residual security risks that are not mitigated.

2. A sample accreditation letter is attached as TAB A to Appendix C.

(b) IATO Letter. If the system is not fully accredited, the cognizant DAA may submit IATO stating acceptance of all significant risks under which the Video Teleconferencing Facility (VTF) is currently operating.

1. This letter must identify mode(s) of operation; highest classification level of information being processed; any risks that preclude accreditation, and any ongoing or planned actions to mitigate those risks.

2. A sample IATO letter is attached as Tab B to Appendix C.

(c) Access Approval Document (AAD). Customers who require DVS access at the SECRET and/or TOP SECRET levels must complete an AAD, signed by their DAA.

1. The AAD must identify the COMSEC Account number, CRYPTO type (i.e., KIV-7, KG-194, and/or KIV 19), as well as the required classified level of the key.

2. A sample AAD is attached as Annex C to Appendix C.

(d) Consent to DISA Monitoring & Compliance Assessment. ATO and IATO letters must be signed by a DAA and must include the following statement: "We acknowledge and consent to DISA conducting an initial vulnerability assessment and periodic, unannounced vulnerability assessments on the connected host systems, to determine the security features in place to protect against unauthorized access or attack."

(2) VTF Connectivity Diagram

(a) Diagram identifies all components and system connections in the VTF. It must address both direct and backside connections, to include the customer's MCU connections to other MCUs or VTFs directly or indirectly.

(b) Diagram must identify connections to other video, voice or data networks.

(c) The VTF connectivity diagram must also include all associated devices including video equipment, MCUs, line interface units (LIUs), hubs, routers, guards, firewalls, gateways, modems, encryption devices and backup devices.

(3) Automated Information System (AIS) Concept of Operations (CONOPS), Security CONOPS, and Security Standard Operating Procedures (SOP) must

(a) Describe how administrative security, procedural security, personnel security, and physical security requirements are implemented in the VTF environment.

(b) Identify the data types and classification level of the VTF owner and its cognizant DAA.

(c) Where appropriate, describe customer procedures on how the VTF and video equipment performs periodic processing to transfers between different call classification levels.

(4) Allied Connection Access Policy

(a) DVS provides video services at Controlled UNCLASSIFIED, US-Only SECRET, US-Only TOP SECRET, Allied SECRET, and (if implemented) Allied TOP SECRET levels.

(b) Connections to elements of foreign governments are permissible when the combatant commander, as the sponsoring activity, provides an ATO that identifies the connection and accepts the risk.

(c) Connections to foreign subscriber terminals must be made through the use of approved security devices employed at each foreign connection.

(5) External Connections

(a) A copy of each external connection and/or associated operation agreement affecting the applying VTF must be provided in the form of a memoranda of agreement/understanding (MOA/MOU). If no external connections apply, ATO and IATO letters must contain statements of non-applicability.

(b) An MOA/MOU is required for each AIS managed by multiple DAAs, e.g. the Navy Video Information Exchange System (VIXS) and must address the accreditation requirements for each DAA involved.

(c) Direct DVS subscribers are responsible for ensuring that all backside connections comply with DVS standards. Where external connections introduce unacceptable risk to the DVS Network, DISA may withhold connection authority, pending a decision by the DSAWG/Joint Staff.

c. Step 3 Processing DVS Request (Packages). After all required information has been submitted to the DISN Video Services Division (NS55), each DVS request package will be reviewed, entered into the Video Services database, and forwarded to the DVS Contractor for continued processing and connection.

3. Exercises. Commanders who require DVS subscriber terminals to support an exercise must provide the above information at least 60 days prior to its scheduled commencement.

4. COMSEC Key. DVS subscribers are required to coordinate with their supporting COMSEC custodians/managers to ensure that DISA NS55 authorizes issue of required KG-194 or KIV-7HS keys.

5. Reporting System Changes. When any significant change is made to a DVS VTF terminal environment, accreditation status, security posture, foreign access and/or backdoor/backside commendations, the responsible commander must submit appropriate information to the DISN Video Services Division.

6. DVS Termination. HQ DISA (NS55) reserves the right to deny or discontinue DVS access to any network, system or terminal demonstrating behavior that increases risk to the DISN infrastructure and/or its subscribers and for non-compliance with the DVS connection requirements.

7. Risk Review

a. Any DVS connection that introduces unacceptable risk must be reviewed by the DSAWG, which may be contacted via a CC/S/A point of contact.

b. The Chief, DISN Video Services will notify Commanders responsible for DVS terminals that exhibit unacceptable risk.

8. Security Awareness & Training

a. Each DVS customer must have an active security awareness and training program for all terminal users, system and security administrators and managers.

b. Security training and awareness programs must be conducted according to guidance applicable to the local support unit and, at a minimum, the requirement of Section 5 (Federal Computer System Security Training) of Public Law 100-235, the Computer Security Act of 1987 (reference s).

9. Incident Reporting

a. Each DVS customer must be capable of detecting unauthorized activity and must have effective procedures for responding to discovered insecurity incidents.

b. Each DVS subscribe terminal site must also have procedures for responding to incidents detected through audit data reviews, such as break-ins at DVS terminals, viruses, Trojan horses and other attacks, such as flooding and protocol spoofing.

c. DVS subscribers must also remain current with respect to security patches and updates, in accordance with established Information Assurance Vulnerability Assessment Program that apply to the DISN connection security device and must maintain a secure configuration management environment.

10. Site Inspections. Under authority granted by the US Military Communications Electronics Board, HQ DISA (NS55) reserves the right to conduct announced site compliance inspections of DVS terminals. Responsible commanders will be notified at least two weeks prior to each such inspection.

11. Re-certification & Approval. Re-certification of all VTC systems connected to DVS is required every three years, for sites operating under ATOs, and every year for those sites operating under IATOs. This complies with policies stated in DOD Directive 8500.1 (reference e), Automated Information Systems Security Requirements, and DOD Instruction 5200.40 (reference f). Re-certification letters will be forwarded to the DISN Video Service Division, NS55.

12. Requests for Service. DVS customers must submit RFS letters to their supporting TCO for issuance of Telecommunications Service Requests (TSRs), IAW DISA Circular (DISAC) 310-130-1 (reference t).

ANNEX A TO APPENDIX C TO ENCLOSURE C

SAMPLE AUTHORIZATION TO OPERATE MEMORANDUM

EXAMPLE ONLY

EXAMPLE ONLY

Combatant Commander/Service/Department/Agency
Letterhead

(Date)

MEMORANDUM FOR: Director, Defense Information Systems Agency
ATTN: NS55

SUBJECT: Accreditation of Defense Information System Network (DISN) Video Services (DVS) Subscriber Terminal (or system)

REFERENCE:
(a) (CC/S/A) Instruction XXX-XXX-XXX, Subject: ---, dated ----.
(b) Accreditation Support Documentation for DVS subscriber terminal located at (address, building and suite/room), dated ----.

1. In accordance with provisions of reference (a), authorization is hereby granted for operation of a DVS subscriber terminal (or system) supporting (Command/Element Name) and located at (address, building and suite/room). This accreditation is based on a review of the information provided in reference (b). It is only valid if the Baseline Security Safeguards defined in the (CC/S/A) specific security guidelines are implemented at the named DVS terminal (or system). That terminal (or system) is authorized to operate in the threat environment defined in reference (b) and with the vulnerabilities identified in applicable (CC/S/A) Baseline Security documents. The accredited terminal (or system) consists of (list equipment). It is authorized to process information classified (specify maximum classification) and below. The named terminal (or system) is connected to DVS and (name any other network(s) to which the terminal is connected).

2. This accreditation is valid for three years from the date of this memorandum. Reaccredidation is required sooner, if there are any significant changes that affect the security posture of the terminal (or system) It is the responsibility of the commander or senior official in charge of the terminal (or system) to ensure that any change in threat,

vulnerability, configuration, hardware, software, or connectivity or other modification is analyzed to determine its impact of terminal (or system) security. Appropriate safeguards will be implemented to maintain a level of security commensurate with the requirements of this accreditation.

(Signature)
Designated Approving Authority
CC/S/A

Copy to: (Commander/Official responsible for operating the named terminal (or system))

ANNEX B TO APPENDIX C TO ENCLOSURE C

SAMPLE INTERIM APPROVAL TO OPERATE MEMORANDUM

EXAMPLE ONLY

EXAMPLE ONLY

Combatant Commander/Service/Department/Agency
Letterhead

(Date)

MEMORANDUM FOR: Director, Defense Information Systems Agency
ATTN: NS55

SUBJECT: Interim Approval to Operate Defense Information Network (DISN) Video Services (DVS) Subscriber Terminal (or System)

REFERENCE:
(a) (CC/S/A) Instruction, Subject ----, dated ----.
(b) Accreditation Support Documentation for DVS subscriber terminal located at (address, building, and suite/room) dated ----.

1. In accordance with the provisions of the reference (a), an Interim Approval to Operate (IATO) is hereby granted to operate a DVS subscriber terminal (or system) supporting (Command/Element Name), located in (address, building, and suite/room). This IATO is based on a review of the information provided in reference (b). It is only valid if the Baseline Security safeguards defined in (CC/S/A) are implemented at the named DVS terminal (or system). That terminal (or system) is authorized to operate in the threat environment defined in reference (b) and with the vulnerabilities identified in applicable (CC/S/A) Baseline Security documents. The named terminal (or system) consists of the following (equipment list). It is authorized to process information (specify maximum classification) and below. The named terminal (or system) connected to the DVS and (name any other network(s) to which the terminal is connected).

2. This IATO is valid for ninety days (**not to exceed 1 year**) from the date of this memorandum. It terminates sooner, if there is any change that affects the security posture of the terminal (or system). Final

accreditation action is required before the expiration of this IATO. It is the responsibility of the commander or senior official in charge of the terminal (or system) to ensure that any changes in threat, vulnerability, configuration, hardware, software, or connectivity or other modification is analyzed to determine its impact on terminal (or system) security. Appropriate safeguards will be implemented to maintain a level of security consistent with the requirements of this IATO.

(Signature)
Designated Approving Authority
Combatant

Commander/Service/Department/Agency
Copy to: (Commander/Official responsible for operating the named terminal (or system))

ANNEX C TO APPENDIX C TO ENCLOSURE C

SAMPLE ACCESS APPROVAL DOCUMENT (AAD)

EXAMPLE ONLY

EXAMPLE ONLY

Access Approval Document (AAD)

Must Be Completed For Cryptographic Transmission
Revised: 4 March 2003

Site ID* ____________________ Date ______________
Installation ____________________________
Location/Room # ____________________________
Bldg./Street ____________________________
City ____________ State _________ _________

This document must be completed prior to your facility being able to conduct classified videoconferences. Answering No or not answering any of the following questions may prevent your site from conducting classified videoconferences.

Organization Message Address ____________________________
i.e. DISA WASHINGTON DC//NS55//
Comsec Message Address ____________________________

COMSEC Account #_________ LMDKP? Yes □ NO □ (ok to mark no)

CRYPTO Type: KIV-7/HS □ KG-194 □ KIV-19 □ Tactical? Yes □ No □

Defense Courier Service (DCS) 2 line address ________________________
____

COMSEC Custodian Name____________________________

Phone # __________________ Email

COM/DSN if available

1. Provide DISA NS55 a signed copy of the Authority to Operate (ATO) either interim or final, a site diagram and this completed AAD.

2. Classification level: (Mark all that apply) Unclassified □ US Secret □ US Top Secret □ KIV-7 Allied Secret □ Canada □

VTC Facilitator Name ________________________

Phone # ________________________ Email ________________________

Designated Approval Authority (DAA):

Title ________________________ Grade ____________

Phone # ____________ Email ________________________
COM/DSN if available

Name ________________________ ________________ __________
Signature Date

I (DAA) certify the VTC facility listed above is authorized to operate at the requested classification level. "We acknowledge and consent to DISA conducting an initial vulnerability assessment and periodic unannounced vulnerability assessments on the connected host systems to determine the security features in place to protect against unauthorized access or attack."

* This must be filled in. If you currently have a site ID, enter it here. For a new Site ID please coordinate with DISN Video Services (DSN 312-761-1376, Com 703-681-1376).

Access Approval Document

Certification / Accreditation Information
Page 2 of 2

Designated Approval Authority:
The Designated Approval Authority (DAA) is the Command sponsored local element / entity assigned the responsibility of determining, based on the risks, if a videoconferencing system, network, or information management system can be operated in a classified mode.

You are requested to maintain this document at your site. DISN Video Services (NS55) and authorized representative (EU52 for Europe, PC52 for PAC), must have a signed copy prior to service activation and crypto key distribution.

POC this action is:

For CONUS: DISN Video Services Division (NS55), cml. (703) 882-3248, DSN 381-3248
For Europe: DISA EUR (EU52), cml. 011-49-711-68639-5840/5260, DSN 314-434-5840/5260
For PAC: DISA PAC (PC52), VTC OPS, cml. 808-656-0196, DSN 315-456-0196

Fax AAD, ATO and Site drawing to:
** For CONUS/OCONUS:
DISN Video Services Division (NS55)
5275 Leesburg Pike
Falls Church, Virginia 22041-3801
Fax (DSN) 312-381-3249
(Com) 703-882-3249

For EUROPE: DISA Europe/ Attn: EU52
Unit 30403
APO AE 09131
Fax (DSN) 314-434-5312
(Com) 011-49-711-68639-5312

For PAC: DISA PAC – Attn: PC52, VTCOPS
Bldg 107
Wright Avenue
Wheeler AAF
Hawaii 96854-5120
Fax (DSN) 315-456-3838
(Com) 808-656-3838
** AAD is faxed to NS55 for all areas CONUS/OCONUS

(INTENTIONALLY BLANK)

APPENDIX D TO ENCLOSURE C

VALIDATION AND APPROVAL REQUEST FOR DOD CROSS DOMAIN, NON-DOD GOVERNMENT, CONTRACTOR OR FOREIGN ENTITY CONNECTIONS

1. Connection requests for DOD cross domain, non-DOD government (federal, state, local), contractor or foreign entity connections require validation and approval of operational requirement. Submit this validation and approval request before or simultaneously with the connection request.

2. DOD Cross Domain Connection. Following connections validation and approval requirements are mandatory for cross domain connections to SIPRNET or other DOD US classified security domain or unclassified enclaves/networks.

a. Sponsoring organization endorses the connection validation request (see TAB A for Request Example) and forwards to Joint Staff, J-6.

b. Joint Staff, J-6 validates and approves the connection request.

c. Joint Staff, J-6 informs DISA of validation and approval of operational requirement.

3. Foreign Connection. Following connection validation and approval requirements are mandatory for direct or indirect connections between US classified or unclassified enclaves and foreign entity. This includes US classified or unclassified enclaves to US classified or unclassified enclaves, which permit direct foreign access or connections of US classified or unclassified enclaves to US enclaves, which are connected to other shared classified or unclassified enclaves (e.g., coalition, bilateral).

a. Sponsoring DOD CC/S/A organization prepares the connection validation request (see TAB A for Request Example) and forwards to appropriate Combatant Command.

b. Combatant command reviews and endorses sponsoring organization (Service or Defense Agency) connection request. If foreign entity country is located outside requesting combatant command AOR, appropriate combatant command will be provided information copy of request. Combatant command forwards request to Joint Staff, J-6.

c. Joint Staff, J-6, validates and approves connection request.

d. Joint Staff, J-6, informs DISA of validation and approval of operational requirement.

e. Sponsoring DOD organization is responsible for ensuring compliance with all DOD IA and CND policies and procedures.

4. Non-DOD Government Connection. Following connections validation and approval requirements are mandatory for connections between DOD and non-DOD government information systems.

a. Sponsoring organization endorses the connection validation request (see TAB A for Request Example) and forwards to Joint Staff, J-6.

b. Joint Staff, J-6, validates the connection request and forwards to ASD(NII).

c. ASD(NII) approves the connection request and informs Joint Staff, J-6.

d. Joint Staff, J-6, informs DISA of validation and approval of operational requirement.

e. Non-DOD USG organization must comply with all DOD IA and CND policies and procedures.

f. The operational requirement for non-DOD government connections will be revalidated by sponsoring DOD organization within 30 days of expiration of original validation.

g. Sponsoring DOD organization agency is responsible for ensuring funding is arranged for the connection.

h. Connection must be physically segregated from the non-DOD government infrastructure.

i. DOD sponsor conducts annual on-site security reviews.

5. Contractor Connection. Following connection validation and approval requirements are mandatory for connections between DOD and

Contractor information systems:

a. Sponsoring DOD organization endorses the connection request (see TAB A for Request Example) and forwards to Joint Staff, J-6.

b. Joint Staff, J-6, validates the connection request and forwards to ASD(NII).

c. ASD(NII) approves the connection request and informs Joint Staff, J-6.

d. Joint Staff, J-6, informs DISA of validation and approval of operational requirement.

e. Contractor must comply with all DOD IA and CND policies and procedures.

f. Sponsoring DOD organization agency is responsible for ensuring funding is arranged for the connection.

g. Connection must be physically segregated from the corporate infrastructure.

h. Government sponsor conducts annual on-site security reviews.

(INTENTIONALLY BLANK)

ANNEX A TO APPENDIX D TO ENCLOSURE C

CROSS DOMAIN VALIDATION AND APPROVAL REQUEST MEMORANDUM

Memorandum Example: The following memorandum provides an example request with required information for connection of non-DOD USG, contractor or foreign access. Send the memorandum to the Joint Staff, J-6, ATTN: J-6T, Washington, D.C. 20318-6000. Note: Substitute appropriate network (e.g., NIPRENT or DVS) for SIPRNET in memo.

EXAMPLE ONLY

Defense Threat Reduction Agency
45045 Aviation Drive
Dulles, VA 20166-7517

EXAMPLE ONLY

14 Feb 03

FROM: DTRA-SWET

MEMORANDUM FOR: Joint Staff/J6T (Attn: Major David Phillips, RM 1D770)

SUBJECT: Secret Internet Protocol Network (SIPRNET) Connectivity for the Federal Emergency Management Agency (FEMA)

1. CONNECTION REQUIREMENT: Request a T-1 SIPRNET connection at FEMA's office in Raliegh, NC, and two alternate operating locations in Salem, Oregon and Miami, Florida, to support the Integrated Munitions Effects Assessment (IMEA) program.

2. DISCUSSION: The Defense Threat Reduction Agency (DTRA) has developed a tool to aid the weaponeer in defeating high value targets containing weapons of mass destruction. The tool, IMEA, was developed to fill a need arising from the Gulf War. It is fast-running and capable of running on a portable, relatively low-end machine. Our customer base has grown to nearly 300 users world-wide since the product's first release three years ago. This year we will be installing a web page on the SIPRNET to allow users to post problem reports, communicate with the developer, and obtain other information to facilitate warfighter use. FEMA has been tasked to trouble-shoot and resolve user problems on a real-time basis, and, if needed, to operate 24 hours per day in a help-desk mode. It is, therefore, essential that they have access to the SIPRNET at these three locations to support DTRA.

3. MISSION PARTNERS AND OPERATIONAL JUSTIFICATION:

a. DOD Sponsor Unit: DTRA

b. DOD Sponsor Mission: Provide weaponeering solution with IMEA in support of the warfighter. Develop and analyze crisis planning and provide critical problem resolution support in near real time.

c. Non-DOD agency/Contractor: FEMA

d. Non-DOD agency/Contractor DOD operational requirement:

1. Secure Development – At times, the weaponeer will need assistance in developing a weaponeering solution with IMEA. During crisis planning, quick problem resolution is critical. In order to assist the user in a timely manner, FEMA may ask them to send us their work via the SIPRNET for analysis. We will provide advice to the user. If problems reside in the programming code, FEMA will develop and distribute the fix via the SIPRNET.

2. Exercise Support – FEMA and DTRA routinely supports Combatant Command exercises throughout the world. As in crisis planning, there may be problems encountered while trying to weaponeer a target. Problems may involve techniques to model complex targets or developing unique work-arounds to compensate for unusual situations. Our office is best suited to provide the modeling support, to analyze programming problems, and to develop fixes.

c. Project and expiration: Access for IMEA is required for four years until 30 Dec 2007.

d. Contract # and expiration: N/A.

e. CAGE CODE and RTRP #: XJ4D23J, #3041.

f. Funding Source: FEMA provided.

g. Accreditation Authority:

4. CONNECTION LOCATION(S)/ADDRESS:

a. FEMA HQ, 1234 Kitty Hawk Blvd, Raleigh, NC 28817

b. FEMA Detachment 51, 5000 Mountain Drive, Salem, OR 95801

c. FEMA Detachment 23, 2121 Aquarius Ct, Miami, FL 33521

5. EXTERNAL ACCESS REQUIRED:

a. Applications/Databases: IMEA, Intellink-S, and NORTHCOM Web site

b. Protocols: Web and Mail

c. Specific IP addresses: 198.99.99.2, 201.87.87.81, and 56.94.84.64

d. DOD Installations: Ft. Meade, MD and HQ SOUTHCOM

6. CONCLUSION: Approval of this request will provide for an efficient and economical way for FEMA to support DTRA and the warfighter in crisis and deliberate planning missions as well as provide for an efficient method to release and update future versions of IMEA.

7. POINTS OF CONTACT (POCs):

a. DOD Sponsor: DTRA POC is Mr Steve Sipperer, commercial (704) 223-8374, fax (704) 223-9001, e-mail SippereS@dtra.mil.

b. Non-DOD Agency/ Contractor: FEMA representative is Mr. Clint Black, commercial (618) 878-2305, e-mail is Clint.Black@fema.gov.

c. Security: FEMA Information Systems Security Officer (ISSO) is Ms Peggy Palmer, commercial (618) 878-7373, fax (618) 878-8399, e-mail is PalmerPe@fema.gov.

LEON R. DONAHUE, GS-15
Program Manager, Special Weapons
Targeting

(INTENTIONALLY BLANK)

APPENDIX E TO ENCLOSURE C

DISN SECURITY INFORMATION ASSURANCE PROGRAM

1. Background. The DISN Security Information Assurance program integrates CC/S/A and DISA inspection and assistance visit programs to assess DISN security status. DISA will support CC/S/As through site visits or remote monitoring and vulnerability assessments.

2. Inspections and Visits

a. Site Inspections/Visits. The program consists of three levels of on-site inspections: compliance inspections, assistance visits and technical engineering inspections/visits. Organizations will integrate types of inspections/visits described below to determine enclave and connection posture. The inspection assets will range from non-technical teams with a systemic orientation to highly technical oriented teams. Examples of assets to conduct on site inspections are Inspectors General (IG), Cross Domain, and various assistance teams.

(1) Compliance Inspections. Compliance inspections include organizations/team (e.g., CC/S/A Inspector General, auditors and DSS) that provide a systemic perspective of several aspects of information assurance; and provide local accrediting authorities a basis for immediate improvement.

(a) Compliance inspections are performed during scheduled visits.

(b) The primary focus is on documentation and the synchronization between local information and centralized repositories maintained by CC/S/A and DISN network operators; training and certification deficiencies; network and enclave documentation and systemic issues.

(2) Assistance Visits. Assistance visits include organizations/teams (e.g., CC/S/A IA organizations and DSS) able to identify and evaluate more complex security issues, and, along compliance visit results, provide basis for assessing information assurance training, implementation and operation.

(a) Assistance visits support CC/S/A respective Information Assurance programs, the Services and Agencies conduct assistance visits.

(b) Assistance teams are more technically focused. The teams provide assistance in correcting deficiencies noted by compliance teams, assess operational procedures and practices, and evaluate documentation and information handling. The primary focus is to identify and resolve deficient operational practices and procedures as well as device configuration issues.

(c) Assistance teams validate previous compliance inspection results and assist in resolving remaining deficiencies. Repository synchronization will also be accomplished. Unresolved training and certification deficiencies will be noted for resolution within Service and Agency channels.

(3) Technical Engineering Inspections. Technical Engineering inspections include organizations/teams (e.g., CC/S/A teams, CDTAB and SIPRNET Inspection Team) that provide assurance that trusted devices continue to be maintained and operated in a manner that minimizes community risk, and provide training where necessary.

(a) Technical Engineering inspections (e.g., JVAP) primarily focus on the secure engineering, implementation, and, where applicable, operation of devices that move information across classification boundaries.

(b) Teams validate previous compliance inspections and assistance visit results and resolve remaining deficiencies where possible.

3. Remote Monitoring and Vulnerability Assessments. Remote monitoring and vulnerably assessments develop a profile of potential configuration vulnerabilities and to alert the site. Remote monitoring and vulnerability assessments begin when an enclave is first granted connectivity.

a. DISA (NS52) conducts remote monitoring of enclave and long-haul network operations.

b. Organization providing local and long-haul component will conduct monitoring.

c. Sampling. Sampling is conducted to evaluate quality of service, determine service efficiency, or support engineering actions to improve network performance.

d. Security. Security assessments will examine consistency of site topology documentation and the conformance of network resident devices with vulnerability alerts issued by DOD Computer Emergency Response Team (CERT). The long-haul operator will accomplish this for the SIPRNET, DIA for JWICS, and the Services/Agencies will accomplish for NIPRNET.

4. Inspection Criteria

a. Sample checklists for self-assessments and compliance inspections/visits can be found at web site http://guides.ritchie.disa.mil. The checklists cover both traditional security and information assurance.

b. Site visit inspections should follow published criteria for the respective CC/S/A or criteria for the particular devices when classification boundaries are involved. Criteria will be established during the initial accreditation of the device.

c. The criteria for remote monitoring will be based on published Security Technical Implementation Guides (STIGs), vulnerability notices issued through CERT channels, or other criteria established by the CC/S/A organization conducting the monitoring and provided to monitored sites.

5. Reporting

a. Inspection/visit findings and results will be published through existing command and technical management channels and be available to appropriate CC/S/A.

b. Results reporting for contractors will be to the contract management organization, the contract sponsor, and to long-haul network operator(s) and the supporting information assurance management organization of contractor sponsor.

c. Connection documentation formats should be modified to provide an opportunity for an enclave to report when last inspected and the type of inspection, including self-assessments.

6. Enclave Categorization. Criteria for categorizing an enclave are provided in subparagraph 8. This categorization will support allocating limited technical assets to enclaves having the greatest IA benefit for interconnected community as a whole. Additionally, categorization will be used to establish inspection scope and periodicity (subparagraph 7).

7. Inspection Responsibility and Frequency Table. "DISN Networks Security Inspection Table" (Table C-B-1) summarizes the execution concept for the DISN Security Information Assurance Program.

	NIPRNET		SIPRNET	
Category	Frequency	Inspecting Element	Frequency (Minimum)	Inspecting Element
1	Every 3 Years	IG	Every 3 Years	IG
2	Every 3 Years	CC/S/A	Every 3 Years	CC/S/A
3 (DOD)	Every 2 Years	CC/S/A	Every 2 Years	CC/S/A
3 (Contractor)	Annual	DSS	Annual	DSS
4	Annual	CC/S/A	Annual	DISA

Table C-E-1. DISN Networks Security Inspection Table

8. Enclave Inspection Categories. The following categories will be applied to connected enclaves as a means to allocate scarce technical inspection assets. Categories reflect enclave configurations that potentially impact enclave/network security posture. The categories accommodate who will accomplish the inspection/visit, the criteria used, and the frequency of inspection/visit. Unless specifically referenced the category criteria applies to both NIPRNET and SIPRNET enclaves.

a. Category One

(1) Enclave operates at a single classification level.

(2) Enclave employs a firewall or firewall-like device in place between local area network and wide area network.

(3) Enclave does not support remote access.

(4) Internet service is via DISA-provided gateway for NIPRNET connected enclaves.

(5) No cross domain connections exist for connected enclaves.

b. Category Two

(1) Enclave operates at a single classification level.

(2) Enclave has a firewall in place.

(3) Internet service is via DISA-provided gateway for NIPRNET connected enclaves.

(4) NIPRNET enclave with central dial-in/dial-out modem banks.

c. Category Three

(1) Enclave operates at a single classification level.

(2) NIPRNET enclave with connection to Internet with no firewall or firewall not via DISA-provided gateway.

(3) Contractor facility with NIPRNET connectivity.

(4) SIPRNET enclave without firewalls.

(5) SIPRNET enclave that supports a dial-incapability.

d. Category Four

(1) Any enclave that has cross domain connections that move information between two different classification levels (includes foreign systems).

(2) Contractor site with SIPRNET connectivity.

(3) Any site with non-US personnel integrated into work force/work area with SIPRNET access.

(4) Any site identified by the DISA SCAO as non-compliant in providing requested connection approval documentation, or does not meet the compliance timeline in a failed DISA SCAO remote network

assessment.

9. Joint Vulnerability Assessment Process (JVAP)

a. All sites with an approval to connect to the DISN are subject to an annual on-site JVAP, or as otherwise directed by the Joint Staff.

b. The JVAP is a process using checklists and DISA and NSA procedures to assess specific configurations, operations and administration of the cross domain solution(s). Types of JVAPS:

(1) Scheduled JVAP. Scheduled JVAPs will be performed annually and will be coordinated and scheduled in advance with the enclave DAA and the site POC.

(2) Short Notice JVAP. Short notice JVAPs will be performed as required. This may occur with limited (less than 24 hours) notification and coordination with the enclave DAA and POC.

c. The JVAP verifies the configuration and identifies possible security vulnerabilities of a cross domain solution. A cross domain solution connects two different security domains and restricts the information that transfers between the domains. The security posture and operations of the cross domain solution must comply with approved conditions to maintain connection authorization.

d. A DISA FSO team lead will notify the enclave DAA and the CC/S/A representative for both scheduled and short notice JVAP visits. In cases when the enclave DAA is not available, the CC/S/A representative will be asked to assist in the coordination of the visit.

e. DISA and NSA will perform data collection and analysis on the cross domain solution(s). The collection and analysis will result in a detailed listing of vulnerabilities with recommended corrective actions. DISA will maintain the results in a secure database. The site will be responsible for updating status of corrective action through the enclave DAA. The final report, to include recommended corrective action(s), will be made available to the enclave DAA.

f. High-risk vulnerabilities will be corrected (when possible) prior to the JVAP team leaving the site. The enclave DAA will report the status of remaining vulnerabilities until closed.

ENCLOSURE D

REFERENCES

a. CJCSI 6250.01 Series, "Satellite Communications"

b. CJCSI 6215.01 Series, "Policy for Department of Defense Voice Networks"

c. DCID 6/3 Series, "Protecting Sensitive Compartmented Information within Information Systems"

d. DODI 4640.14, 6 December 1991, "Base and Long-Haul Telecommunications Equipment and Services"

e. DOD Directive 8500.1 Series, "Information Assurance (IA)"

f. DOD Instruction 5200.40, 30 December 1997, "DOD Information Technology Security Certification and Accreditation (C&A) Process"

g. DOD 8510.1-M, 31 July 2000, "DOD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual"

h. DOD 5200.1-R, 14 January 1997, "Information Security Program"

i. DOD Directive 5230.11, 16 June 1992, "Disclosure of Classified Military Information to Foreign Governments and International Organizations"

j. CJCSI 5221.01 Series, "Delegation of Authority to Commanders of Combatant Commands to Disclose Classified Military Information to Foreign Governments and International Organizations"

k. DOD Instruction 8500.2, Series, "Information Assurance (IA) Implementation"

l. DOD Instruction 8540.aa, Draft, "Interconnection and Data Transfer Between Security Domains"

m. CJCSI 6510.01, Series, "Information Assurance (IA) and Computer Network Defense (CND)"

n. DOD 5200.22.M, 1 May 2000, “National Industrial Security Program Operating Manual”

o. DISA Circular 310-130-4, 18 August 1993, “Defense User’s Guide to the Telecommunications Service Priority (TSP) System”

p. CJCSM 6510.01 Series, “Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)”

q. NSTISSI No. 7003, 13 December 1996, “Protected Distribution System”

r. NIST Special Publication 800-37, Version 1.0, October 2002, “Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems”

s. Section 5 (Federal Computer System Security Training) of Public Law 100-235, the Computer Security Act of 1987

t. DISA Circular (DISAC) 310-130-1, 4 April 2000, “Submission of Telecommunications Service Requests”

u. NSTISSI 4009, September 2000, “National Information Systems Security Glossary”

v. Defense Information System Network (DISN) Long-Haul Block Security Policy, May 1999

w. JROCM 047-95, 30 March 1995, “Defense Information System Network (DISN) Mission Need Statement (MNS)”

x. JROCM 048-96, 15 April 1996, “Validation of Defense Information System Network (DISN) Capstone Requirements Document”

GLOSSARY

PART I--ABBREVIATIONS AND ACRONYMS

A

AAD	Access Approval Document
AIS	automated information system
AM	account manager
AOR	area of responsibility
ASD(NII)	Assistant Secretary of Defense for Networks and Information Integration
ATC	Authority to Connect
ATO	Approval to Operate

C

CC/S/A	Combatant Command, Service and Defense Agency
C4I	command, control, communications, computers and intelligence
CAP	connection approval process
CDA	Cross Domain Appendix
CDIO	Cross Domain Implementation Office
CDIP	Cross Domain Interface Process
CDSO	Cross Domain Solutions Organization
CDSAP	Cross Domain Solutions Assessment Panel
CDTAB	Cross Domain Technical Advisory Board
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CISA	Communication Information Service Activity
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CJCSM	Chairman of the Joint Chiefs of Staff manual
COMSEC	communications security
CONOPS	concept of operations
COP	common operational picture
CTF	coalition task force
CTM	Consent to Monitor

D

DAA	Designated Approving Authority
DBOF	Defense Business Operating Fund
DCID	Director of Central Intelligence Directive
DIA	Defense Intelligence Agency

DICAST	Defense and Intelligence Community Accreditation Support Team
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DITSCAP	DOD Information Technology Security Certification and Accreditation Process
DOD	Department of Defense
DRSN	Defense Red Switch Network
DSAWG	DISN Security Accreditation Working Group
DSN	Defense Switched Network
DSS	Defense Security Service
DTRA	Defense Threat Reduction Agency
DVS	DISN Video Services
DVS-G	DISN Video Services-Global

F

FEMA	Federal Emergency Management Agency
FSO	Field Security Office

G

GCCS	Global Command and Control System
GIAP	GIG interconnection approval process
GIG	Global Information Grid

I

IA	information assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IAPB	Information Assurance Policy Board
IATC	interim authority to connect
IATO	interim authority to operate
IAW	in accordance with
IC	Intelligence Community
IG	Inspector General
IMEA	Integrated Munitions Effects Assessment
IMR	Initial Modeling Request
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
IT	information technology

J

JTF	joint task force
JVAP	Joint Vulnerability Assessment Process
JWICS	Joint Worldwide Intelligence Communications system

	L
LIU	line interface unit
	M
MCEB	Military Communication Electronics Board
MCU	multipoint control unit
MOA	memorandum of agreement
MOU	memorandum of understanding
	N
NCAO	NIPRNET Connection Approval Office
NIPRNET	Non-Classified Internet Protocol Router Network
NSA	National Security Agency
NSEP	National Security Emergency Preparedness
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
	O
OSD	Office of the Secretary of Defense
	P
PAT	process action team
PDS	protected distribution system
POC	point of contact
	R
RFS	request for service
	S
SAA	SIPRNET Access Assessment Questionnaire
SABI	SECRET and Below Interoperability
SCAO	SIPRNET Connection Approval Office
SCI	sensitive compartmented information
SIPRCAP	SIPRNET Connection Approval Process
SIPRNET	SECRET Internet Protocol Router Network
SOP	standard operating procedures
SSAA	System Security Authorization Agreement
STIGs	Security Technical Implementation Guides
	T
TCO	Telecommunications Certification Office
TSP	Telecommunications Service Priority
TSR	telecommunications service request

	U
USG	United States Government
USSTRATCOM	US Strategic Command
	V
VIXS	Video Information Exchange System
VMS	Vulnerability Management System
VTF	Video Teleconferencing Facility

PART II--DEFINITIONS

accreditation. Formal declaration by a Designated Approving Authority (DAA) that an information system (IS) is approved to operate in a particular security mode at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards. (NSTISSI 4009, reference u)

authentication. Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. (DOD Directive 8500.1, reference e)

certification. Comprehensive evaluation of the technical and non-technical security safeguards of IS to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements. (NSTISSI 4009, reference u)

Common Criteria. The International Common Criteria for Information Technology Security Evaluation (CC) defines general concepts and principles of information technology (IT) security evaluation and presents a general model of evaluation. It presents constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems. (DOD Instruction 8500.2, reference k)

Community. Data and system owners who are affiliated by information system interconnection. (DOD Instruction 8540.aa, reference l)

community risk. Probability that a particular vulnerability will be exploited within an interacting population and adversely impact some members of that population. (DOD Directive 8500.1, reference e)

connected network. Any network or enclave that is physically or logically interfaced with the local DAA's enclave is considered connected to that network.

connection approval. Formal authorization to interconnect information systems. (DOD Directive 8500.1, reference e)

cross domain solution. An information assurance solution that provides the ability to manually and/or automatically access and/or transfer between two or more differing security domains.

data. Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representation, such as characters, or analog quantities, to which meaning is or might be assigned. (DOD Instruction 8500.2, reference k)

Defense Information System Network (DISN). The DOD consolidated worldwide enterprise-level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations. (DOD Directive 8500.1, reference e)

designated approving authority (DAA). The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Accrediting Authority and Delegated Accrediting Authority. (DOD Directive 8500.1, reference e)

DISN user. An individual assigned to an organization having devices directly or indirectly connected to the DISN.

DISN Security Accreditation Working Group (DSAWG). Provides, interprets, and approves DISN security policy, guides architecture development, and recommends accreditation decisions to the DISN Flag panel.

DOD CIO Executive Board Charter for Adjudication of Requests for Waiver of DISN. The DOD CIO Executive Board is the single DOD executive level providing senior management recommendations and decision support for adjudication of requests for waiver of the DISN. The board is supported by the GIG Waiver Review Panel.

DOD information system. Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced IT-based processes, and platform IT connections. (DOD Directive 8500.1, reference e)

DOD Information Technology Security Certification and Accreditation Process (DITSCAP). The standard DOD approach for identifying information security requirements, providing security solutions, and managing information system security activities. (DOD Instruction 5200.40, reference f)

Defense Intelligence Community Accreditation Support Team (DICAST). Supports the intelligence principal accreditation authorities (PAAs), which includes, the Director of the NSA, the Director of the DIA, the Director of the NRO, or the Executive Director of the Central Intelligence Agency. The responsibilities of the DICAST are outlined in DCID 6/3 (reference c).

enclave. Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the AIS applications or outsourced IT-based processes they support, and derive their security needs from those systems. They provide standard IA capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and electronic mail. Enclaves are analogous to general support systems. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers. (DOD Directive 8500.1, reference e)

End-to-End. The fusion of all requisite components to deliver a defined capability. For the GIG, this implies all components from the user access and display devices and sensors to the various levels of networking and processing, all associated applications, and all related transport and management services. For the DISN services, end-to-end encompasses service user to service user (e.g., PC-to-PC, phone-to-phone).

Global Information Grid (GIG). Globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems (NSS) as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all DOD, National Security, and related Intelligence Community (IC) missions and functions (strategic, operational, tactical and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DOD users and systems. Non-GIG IT is stand-alone, self-contained, or embedded IT that is not or will not be connected to the enterprise network. The GIG includes any system, equipment, software, or service that meets one or more of the following criteria:

Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services.

Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.

Processes data or information for use by other equipment, software, and services. (DOD Instruction 8500.2, reference k)

GIG Interconnection Approval Process. Electronic process to submit connection information and register a GIG connection.

guards. Process limiting the exchange of information between systems. (NSTISSI 4009, reference u)

information assurance. Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (DOD Directive 8500.1, reference e)

interconnected. An *interconnected* information system is composed of *separately accredited* information systems (i.e., Enclaves). Each self-contained information system maintains its own intra-system services and controls, protects its own resources, and retains its individual accreditation. Each participating information system has its own IAO (ISSO). (DOD Instruction 8540.aa, reference l)

Joint Vulnerability Assessment Process (JVAP). A process using checklists and DISA/NSA procedures to assess specific configurations, operations and administration of the cross domain solution(s).

Protection Profile. A protection profile contains a set of security requirements either from the Common Criteria for Information Technology Security Evaluation (CCITSE), or stated explicitly, which should include an Evaluation Assurance Level (EAL). The protection profile permits the implementation independent expression of security requirements for a set of Targets of Evaluation (TOEs) that will comply fully with a set of security objectives.

Risk Decision Authority Criteria. Criteria for identifying an acceptable level of community risk appropriate for the connection approval authorities to employ in making connection decisions.

robustness. A characterization of the strength of a security function, mechanism, service or solution, and the assurance (or confidence) that it is implemented and functioning correctly. DOD has three levels of robustness:

high robustness. Security services and mechanisms that provide the most stringent protection and rigorous security countermeasures.

medium robustness. Security services and mechanisms that provide for layering of additional safeguards above good commercial practices.

low robustness. Security services and mechanisms that equate to good commercial practices. (DOD Directive 8500.1, reference e)

security domain. Within an information system, the set of objects that is accessible. Access is determined by the controls associated with information properties such as its security classification, security compartment or sensitivity. The controls are applied both within the information system and in its connection to other classified or unclassified information systems. (DOD Directive 8500.1, reference e)

security markings. Indicators applied to a document, storage media, or hardware component to designate categorization and handling restrictions applicable to the information in the document. For intelligence information, these could include compartment and sub-compartment indicators and handling restrictions. For DOE information, these could include indicators of information type (such as Restricted Data), and Sigma categories. (DCID 6/3, reference c)

security penetration testing. System testing designed to evaluate the relative vulnerability of the system to hostile attacks. Penetration testers often try to obtain unauthorized privileges (especially attempts to obtain “root” or “superuser” privileges) by exploiting flaws in system design or implementation. (DOD Instruction 8540.aa, reference l)

single level connection. Connection of enclaves of like security domains.

subnetwork. A logical partition of a network amenable to separate management, control, and provisioning because of functional or geographic reasons.

type accreditation. Type Accreditation. In some situations, a major application or general support system is intended for installation at multiple locations. The application or system usually consists of a common set of hardware, software, and firmware. Type accreditations are a form of interim accreditation and are used to certify and accredit multiple instances of a major application or general support system for operation at approved locations with the same type of computing environment. (NIST Special Pub 800-37, reference r)

validation. Determination of the correct implementation in the completed IT system with security requirements and approach agreed on by the users, acquisition authority, and the DAA. (DOD Instruction 5200.40, reference f)